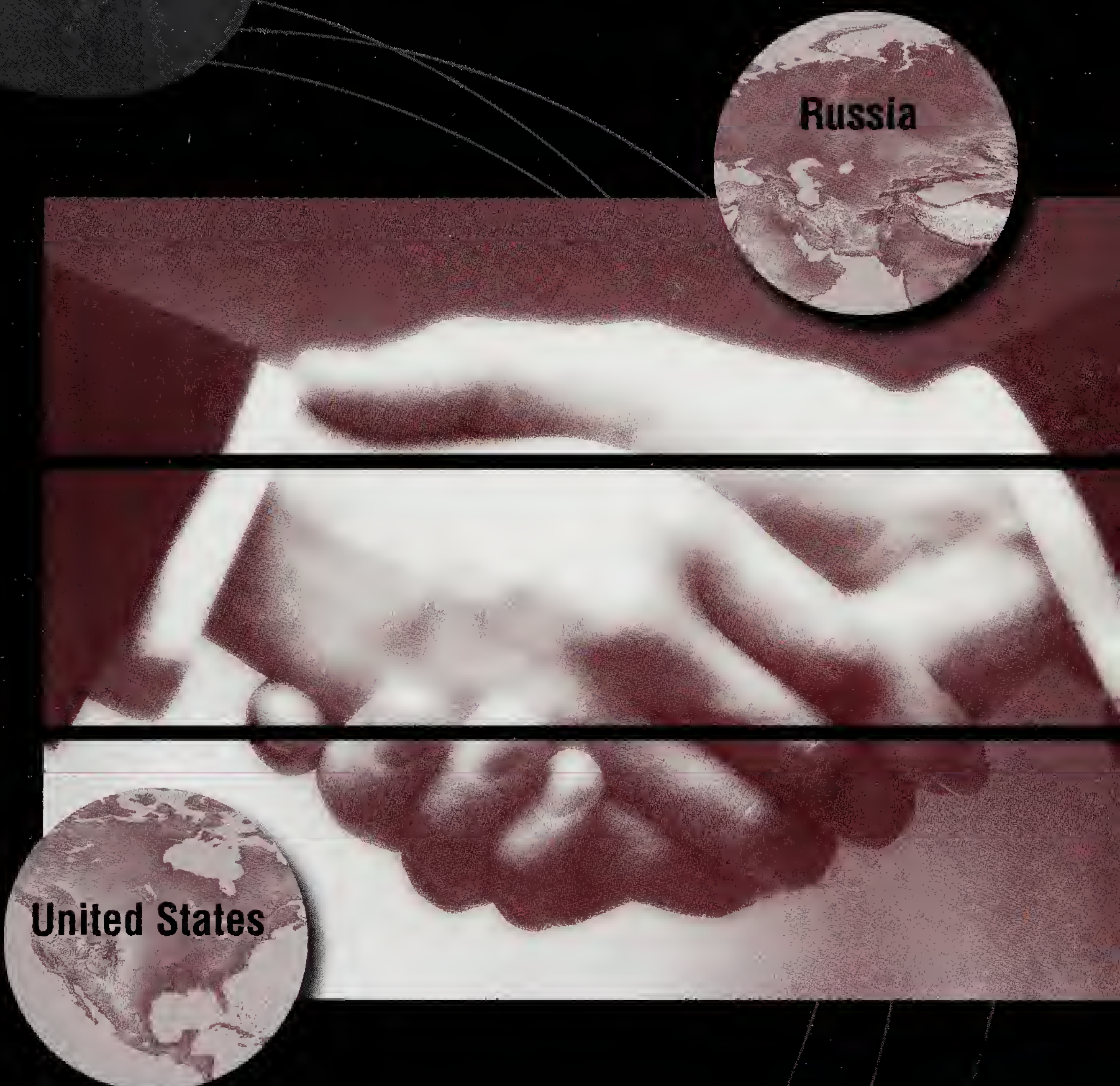
C3

Nuclear Command, Control Cooperation



Valery E. Yarynich

The Center for Defense Information is a non-partisan, non-profit organization committed to independent research on the social, economic, environmental, political and military components of global security. To ensure the ability to provide objective analysis, CDI accepts no government or defense industry funding. Its central aim is to educate the public and inform policymakers about issues of security policy, strategy, operations, weapon systems and defense budgeting, and to produce creative solutions to the problems of today and tomorrow. To encourage the intellectual freedom of the staff, CDI does not hold organizational positions on public policy issues. Instead, staff members are dedicated to the concept that the public and political leaders can, and will, make wise choices on complex security matters when provided with facts and practical alternatives.

Center for Defense Information
1779 Massachusetts Avenue, NW
Washington, D.C. 20036-2109

My dear friend
Dr. Bruce Blair
with highest respect,
great gratitude, and
best wishes
from author
January 27,
2004,
Washington D.C.

C^3:

Nuclear Command, Control Cooperation

VALERY E. YARYNICH

CENTER FOR DEFENSE INFORMATION
Washington, D.C.
May 2003

About the Author

Valery Yarynich was born in 1937 to a family of a Soviet Naval officer. He graduated from the Military Academy of Communications, Leningrad in 1959, and began his career in the Strategic Rocket Forces, serving in the very first Soviet ICBM division, near the city of Kirov. From 1966 to 1992, Yarynich was stationed in Moscow, serving in the central command of the SRF until 1986, and spent the last six years of his military career in the General Staff.

His area of specialization is nuclear weapons command and control, and he participated in the design, testing and deployment of the main C^3 systems for silo-based as well as mobile strategic missiles. Most of these systems are in use to this day.

After retiring from the Army, Yarynich worked at the Moscow Institute for World Economy and International Relations, as well as in the Russian State Duma as assistant to Deputy Alexei Arbatov. Since June 2001, Yarynich has been a Visiting Associate Professor at the California State University, San Bernardino.

Yarynich is the author of *Evaluation of A Guarantee* (Moscow State University of International Relations, 1994) and many articles on the issues of arms control and strategic stability in Russian and foreign periodicals.

Acknowledgements

"To all those who worked hard to create nuclear command and control systems"

The publication of this book would have been impossible without the support and encouragement of Dr. Bruce G. Blair. The author is profoundly grateful to Dr. Blair and to the Center for Defense Information for their efforts in its publishing. Many of Bruce Blair's ideas have been put into the foundation of this book.

The author would also like to express his gratitude to the Hon. Thomas C. Reed, Dr. William C. Green, Dr. Frank von Hippel, Dr. Richard L. Garwin, Dr. Nikolai Sokov, Dr. Debbie Ball, Dr. Dean Wilkening and Dr. David Holloway for their valuable ideas.

The author is also grateful to Elena Tsypkin for her translation of the book, to Luba Schwartzman for translating a section of Chapter 4, to Theresa Hitchens, Dan Rothem and Anthony Keats for overseeing the preparation of the book for publication, and to Rachel Freedman for her work on the design.

Support for this project was made available by the John D. and Catherine T. MacArthur Foundation.

Board of Advisors:

Dr. Bruce G. Blair - President, CDI

Table of Contents

Preface

by Dr. Bruce G. Blair,
President, Center for Defense Information

Most Western observers of Russia's system of nuclear control and early warning warn that its deterioration poses a danger to the world. Of particular concern is its questionable effectiveness in preventing the theft of nuclear weapons in storage. That concern animates the West's efforts to assist Russia in securing its vast storehouse of nuclear weapons and raw fissile materials. Other concerns range from the susceptibility of the early warning network to false alarms – increasing the risk of a mistaken launch – to a breakdown of safeguards against unauthorized actions that could lead to an unsanctioned launch of nuclear missiles.

Although Col. (ret.) Valery Yarynich, the author of this volume, shares my view that these are legitimate and reasonable concerns, his assessment diverges considerably on many of the particular points of concern. And his judgment counts a great deal more than mine, and, for that matter, the typical Western observer. Col. Yarynich brings to the discourse some unusual credentials, not the least of which is a 30-year career in the Soviet Strategic Rocket Forces and the Soviet General Staff, where his primary responsibilities lay in streamlining the Russian strategic nuclear command and control system. He is one of a small group of true specialists in this esoteric realm, a person who worked with all the key designers, testers, and implementers of the system.

Having worked closely with Valery and a considerable number of his colleagues in this field for more than a decade, I can attest to his tremendous store of knowledge of the system. From him, and a handful of his colleagues in the military and specialized military industrial design bureaus assigned to build coherent nuclear command-control systems that could carry out orders to execute a large-scale nuclear war and at the same time prevent any accidental or unauthorized use of the Soviet arsenal, I learned a great deal about the Soviet and Russian system that deserves only admiration and confidence.

I learned that the nuclear control system of the Soviet Union and its successor, Russia, is better designed than the nuclear control system of the United States, about which I also have some first-hand, as well as academic, knowledge, having devoted decades of my career to the operation and study of U.S. nuclear weapons. In the adrenalin rush among Western analysts brought on by the fear of a meltdown of Russian nuclear control, a cool analytical understanding of the workings of the Russian system is often missing. There is an impressive side to these workings that has been lost on Western observers, mainly because they have not really grasped the Russian system's architecture.

Whenever I meet with South Asian and other nuclear specialists interested in refining the design of their nascent nuclear command system, I strongly recommend that they examine the Russian system and emulate it if they wish to achieve the highest level of top-down control. The Russian architecture compares favorably with the American because of the extraordinary attention paid to ensuring strict centralized control over Russian (Soviet) nuclear operations. This concentration reflects the core value of Russian political and military culture going back for centuries. From the days of the czars through the dawn of the nuclear age under Stalin and beyond, "control" was the watchword. "Control" is the hallmark of the system, and its pervasive priority is embodied in the most elaborate centralized network the world has ever seen. By comparison, the U.S. system started out as a highly decentralized system that operated on the basis of a great deal of trust between the U.S. civilian leadership and the military. Although the U.S. system evolved toward greater centralization with more stringent technical and organizational safeguards against unauthorized use of nuclear weapons, it remains today far less centralized and "tight" than its Russian counterpart. Alas, the maintenance of the Russian system – human, organizational, and technical – has fallen down, preventing it from realizing its design potential.

Col. Yarynich documents the development of the Soviet and Russian system in fine-grained detail. He provides an authoritative account of the system designers, and the technical and organizational arrangements that evolved from the system's inception after World War II until the present day. His descriptions are based on material that exists in the public domain in Russia, the United States, and elsewhere, but material that called for a true expert to integrate into a coherent picture.

The picture that emerges is often fascinating. The stodgy Soviet bureaucracy created, against all odds it would seem, some of the most innovative systems of nuclear control imaginable. To cite one example, the Soviet "Dead Hand," or *Perimetr* system designed by the Impuls bureau in St. Petersburg, under the guidance of Lt. Gen. Varfolomey V. Korobushin, embodies bold concepts of control for dealing with circumstances involving a sudden U.S. missile attack that decapitated the top political and military leadership in the Moscow metropolis. Reminiscent of the "doomsday machine" in the famous Stanley Kubrick movie *Dr. Strangelove*, this Soviet innovation was placed into operation in the early- to mid-1980s during the nuclear confrontation of the Reagan era.

Col. Yarynich describes the project's history and rationale, and, in fact, he describes all of the significant systems of nuclear control and early warning that evolved during the past one-half century. This encyclopedic account is by far the definitive work on the subject, not only in terms of the various technical projects but also in terms of their function and performance in the overall system. He provides rigorous assessments of the survivability and capabilities of the separate parts and overall system. He provides the factual and analytical basis for informed judgments on the Russian (Soviet) capability to maintain effective control in various stressful environments ranging from large-

scale enemy nuclear assault, to illicit acts on the inside to misuse Russian nuclear forces, to spoofing or cyber-attack by terrorists.

This work is thus required reading of anyone who wishes to grasp the actual inner workings of the Russian nuclear control system before commenting on its strengths and weaknesses. It is also essential reading for those of us who aspire to move beyond the conventional wisdom that the system is riddled with deficiencies. The gloom and doom may be partially justified but often its misinformed and misguided. And a mastery of the subject generates a fair amount of optimism about the inherent strength of the system as well as an understanding of its potential weaknesses.

Col. Yarynich rightly calls for a searching look at both the U.S. and Russian systems by a group of governmental and non-governmental experts. Such a body of experts sharing information about each system could help allay unjustified fears as well as identify genuine deficiencies requiring fixes. American and Russian experts could learn a great deal from each other, and cooperate in addressing vulnerabilities to deliberate exploitation by terrorists, misguided insiders, or other parties. They could cooperate in finding new ways to reduce the risk of mistaken launch on false warning. They could cooperate in figuring out ways to reduce the danger of mistaken or unauthorized launch by Pakistan, India, or other countries. They could cooperate in numerous ways for noble purposes. This book is a terrific first step in this direction of sharing knowledge and advice.

Introduction

This book discusses command and control of strategic nuclear weapons. Its goal is to facilitate cooperation in this field between official and independent experts in Russia, the United States and other countries, and to make these matters a subject of public discussion.

Today we are facing an obvious absurdity. On the one hand, as far as nuclear weapons themselves are concerned, the United States and Russia have become unprecedentedly open with each other, exchanging information that used to be completely secret during the Cold War. Now publicly accessible computer databases include information about various types of American and Russian ballistic missiles and nuclear warheads, their numbers, characteristics, location, design bureaus and production facilities. Experts on nuclear weapons from various countries hold regular meetings, and special organizations and departments within the power structures of both Russia and the United States have already been established in order to implement signed agreements on cooperation in this area. Regular mutual inspections of military bases, testing ranges and industrial enterprises are being conducted. The result of such decisive steps is evident: the process of nuclear arms reduction has started and is successfully continuing.

By the end of the 20th century, the American strategic forces had about 6,400 nuclear warheads; 54 percent of these warheads were submarine-launched ballistic missiles (SLBMs) (on board the Ohio-class nuclear-powered ballistic missile submarines – or SSBNs – armed with Trident-1 and Trident-2 SLBMs), 33 percent were on silo-based intercontinental ballistic missiles (ICBMs) (Minuteman-3 and the Peacekeeper), and 13 percent on board B-52 strategic bombers armed with air-launched cruise missiles. At the same time, Russia had about 6,600 strategic warheads counted under the terms of START I (5,800 of them were in operational status); 33 percent of these warheads were based on SSBNs, 55 percent on silo-based and mobile ICBMs, and 12 percent were carried by strategic bombers.[1]

At the same time, however, absolute secrecy reigns when it comes to command and control of nuclear weapons (in American terminology, C^3I – command, control, communications and intelligence). Two issues are of greatest importance here. First, what measures have been taken by the nuclear powers against accidental or unauthorized use of nuclear weapons, and how reliable are these measures (known as negative control)? Second, what is the ideology for hypothetical authorized employment of nuclear weapons?

Since these weapons exist, and are likely to continue to exist for the foreseeable future, there must also be a clear system of action for national command authorities (NCA) and combat duty crews at all levels in crisis situations. This is called positive control, the effectiveness of which should be estimated not only from the standpoint of providing robust deterrence against a potential attacker, but should also be viewed through the prism of negative control, which is dominant today.

Unfortunately, cooperation in this field between Russia, the United States and other nuclear powers is practically nonexistent. Data on command and control systems and concepts of use continue to be secret. Experts in C^3I do not meet, and urgent problems are not discussed. This is surprising. Nuclear weapons are not the only problem, and reduction of nuclear arsenals is not the only goal. Establishing global security and preventing any accidents with the nuclear monster are much broader and more important tasks on the long road of reductions. But while the level of nuclear *potential* is gradually declining, the level of *danger* is staying relatively the same. This is because to the common citizen, the end result is the same whether a nuclear conflict involves thousands of warheads or "only" dozens. Such an outcome must be prevented in principle, and this can be done only through the command, control and communication (C^3) system. In peacetime, nuclear weapons themselves only become deadly through a mistake in, or intentional misuse of, their command and control system.

Of course, one cannot assume *a priori* that dangers in this field already threaten the world. Perhaps problems do not exist, or that finding their solution can be postponed. However, ignorance and lack of information concerning these dangers weaken mutual trust and may result in considerable problems in the near future. Logic itself suggests the necessity of increased attention to the influence of command and control factors on strategic stability. There is no reason to wait. "Simple intuition suggests that omitting command parameters from consideration invites miscalculation."[2] Nevertheless, Russia and the United States have taken practically no steps in this direction. Why?

Perhaps it is because the subject of nuclear command and control is justifiably considered one of the most complex and delicate. One cannot blame the leaders of the nuclear powers for not understanding all the nuances of the command and control systems. After all, it is the business of technical experts. But at the same time, those in power, who are fully aware of the exceptional importance of command and control, are concerned about irreversible consequences for their national security in case these particular "cards" in their defense "hand" are played. Thus, it is the combination of two circumstances – fear of making an irreversible mistake, and the realization of their relative incompetence in this technologically complex field – that creates the "blockage at the top." This prevents C^3I experts of various countries from sitting around the same table and coming up with practical proposals to make these systems more secure and reliable.

This book proposes one of the possible approaches to initiating international cooperation on nuclear command and control. The main emphasis is not so much on a

traditional description of C^3 systems and the concepts of their employment, but rather on a logical and mathematical substantiation of the admissibility and necessity for open dialogue in the field of C^3I, within reasonable limits. Openness is the key to solving the numerous problems that stand in the way of strengthening civilian control over nuclear forces. It can be achieved without any risk to national security, and in fact, it may even be advantageous both for global security and economics.

Chapter 1 considers the general principles of nuclear command and control systems and their place and role in nuclear forces. It points to a number of the problems and potential dangers inherent to the operation of these systems, and demonstrates the undesirable consequences of complete secrecy. It proposes one possible approach to overcoming this absurdity, namely conducting combined theoretical studies on the effectiveness and permissibility (from the standpoint of national security) of reasonable mutual openness in nuclear command and control; then, if such effectiveness is proven, taking concrete mutual steps for strengthening strategic stability and global security.

Chapter 2 analyzes the major scholarly works on strategic C^3I. These works investigate practically all the major aspects of nuclear command and control, and emphasize the necessity of command and control when considering strategic stability, disarmament and global security. However, substantiating the necessity and possibility for international cooperation in C^3I needs more attention.

This is addressed in Chapter 3, which describes a logical, mathematical method for solving the problem of cooperation. This method was developed and tested on numerous occasions during the 1990s by the Russian military and academic research institutes, to substantiate the required composition and characteristics of strategic nuclear forces (SNF) and their command and control systems. The main conclusion is that *a nuclear power can, theoretically, be reliably guaranteed to retaliate against an attacker under any conditions*, irrespective of the size of prior preparations by the attacker to avoid retaliation (e.g. improvement of the offensive forces and methods for their employment, strengthening of ballistic missile defense – or BMD – increased survivability under conditions of nuclear war, etc.). The method allows analysts, with an accuracy acceptable for practical purposes, to find a quantitative measure for the probability that the required level of retaliation will be implemented, and to correlate the required values of this index on the effectiveness of SNF (including their command and control system) with necessary expenditures.

This approach is practical only under conditions of mutual openness regarding certain aspects of the C^3 systems. Given the theoretically proven assured retaliation, it is possible to move toward this kind of openness while maintaining national security.

Chapter 4 describes the Russian and U.S. nuclear command and control systems, including their history, organization and operational principles. Despite the fact that the C^3 topic is practically closed in Russia, in recent years a considerable number of independent and official experts described elements of strategic nuclear C^3 system, including their real names, missions and some characteristics. Unfortunately, these

disparate data, presented by Russian authors, do not provide an objective picture of the system as a whole. It is also unfortunate that some of these data, and especially a number of Western publications about the Russian strategic C^3, distort the real picture. Thus, I have undertaken in this book to give the previously published data on the Russian C^3 a certain logical structure. In other words, the readers will find here not only the list and brief description of the C^3 elements, but, more importantly, an explanation as to why these elements have been created, what their roles are in the general C^3 system, and what their impact is on strengthening nuclear deterrence. Some information on the systems' designers and manufacturers is also provided, and future prospects are analyzed. This will help maintain strategic stability and counter uninformed speculation on this crucial subject. These issues are discussed primarily in relationship to the first three components of C^3I: command, control and communications. Considerable attention is paid to the Russian strategic rocket forces (SRF) C^3. Information about C^3 systems for the sea-based and air legs of the nuclear triad, as well as for the SNF as a whole, is less detailed.

There is also a brief description of the U.S. nuclear command and control system.

Chapter 5 contains a comparative analysis of some problems in Russian and U.S. C^3. Using examples of negative control, delegation of authority, "dead hand"-type systems, concepts of nuclear weapons use, etc., the chapter demonstrates that these problems are largely similar for both systems, and that it is better to solve them cooperatively.

Chapter 6 proposes some concrete measures for cooperation between Russian and U.S. C^3 experts. It contains a list of questions in the field of nuclear command and control where unclassified publications, as well as discussions by official and independent experts, should be permitted. Questions regarding areas where such openness is impossible are listed as well.

Analysis of the problems listed above is accompanied by references to opinions, conclusions and proposals contained in works by prominent specialists on the subject, mostly Americans. In general, the author's views, based for the most part on those of Russian scholars, largely support the opinions of non-Russian experts, a fact which suggests considerable potential for cooperation. At the same time, the author proposes several alternatives to the American specialists' views, which can also be seen, positively, as material for beginning a discussion on the development of mutually acceptable recommendations.

As noted above, the abbreviation C^3 means "command, control, *communications*." This retains its meaning throughout the book. The author, however, has decided to change this meaning slightly in the title ("command, control, *cooperation*"), in order to immediately draw the reader's attention to the book's foremost concern.

Chapter 1

Why Should C³ be Taken into Account? Potential Dangers and Problems

1.1 What is C³ ?

The general principles for building and operating a C³ system (we use this term to describe only C³ – command, control and communications) are the same for all nuclear powers.

To use the standard definition, a C³ system is the totality of organs, points and means of command and control. When speaking about "organs," we imply, in addition, that they have executive officials, procedures and doctrines of command and control.

The American literature on C³ frequently employs the following simplified definition of command and control: "The ability to send order requires only one-way links from higher authority to the forces; this is command. The ability to receive feedback on an information channel is necessary for control."[3]

The C³ system for strategic nuclear forces (SNF) is designed to provide the top political leaders with complete command of strategic nuclear weapons and, if necessary, with a monopoly on their use. This is true for nuclear force components – land-based, sea-based and/or air-based nuclear missile systems (their composition differs from one nuclear power to another) – as well as for the infrastructure necessary for their operation.

The main functions of a nuclear C³ system are:

- Control of the technical conditions and combat readiness of nuclear missiles;
- Protection of nuclear weapons, at all levels, from unauthorized or accidental use;
- Providing for the routine operations of subordinated forces and staffs;
- Coordination with other services, organs and structures (early warning system, ballistic missile defense, strategic reconnaissance, anti-aircraft defense, ground forces groups, etc.) in carrying out the missions of the nuclear forces;
- Preparation and correction of plans for combat employment of nuclear forces;
- If necessary, combat use of nuclear weapons, including decision-making procedures, preparation of launch orders, and their transmission to the implementation level.

The exclusive right to authorize use of nuclear weapons belongs to the head of state (president, etc.). The C³ system's main requirements are trustworthiness, speed and ease of operation, and combat stability. All levels of the system, from the top leader-

ship down to the implementation level, have groupings of different types of command facilities (highly protected stationary types, mobile land-based, air-based, etc.). These command facilities have round-the-clock combat watch. They are all systematically linked into an integrated network by the common user algorithm, and technologically linked by communication channels based on different physical principles. Command facilities for the top leadership are equipped to receive signals of a nuclear missile attack. All levels of the C^3 system are equipped with devices to block accidental or intentional actions within the system that can result in an unauthorized missile launch.

In the course of combat watch at high command facilities (General Staff and service commanders in chief of the nuclear triad), the condition of nuclear missiles and troops is constantly monitored, and reports about incidents are received at the level required by the circumstances. All means necessary for preparing and transmitting the order to unblock and launch the missiles are kept in constant readiness. The working algorithm of the high command of C^3 for nuclear retaliation is, in principle, the same for every nuclear power and is as follows:

Warning of a missile attack is sent to the head of state and is simultaneously received at the highest-level command posts. Political leaders are then informed of the attack's nature once it is identified. On the basis of this and previous information, the head of state calls an urgent meeting (using teleconference) with the persons who had been given authority in advance to make decisions about use of nuclear weapons. If a joint decision to use nuclear weapons is made, the head of state uses special technology (the "nuclear briefcase") to prepare the authorization and transmits it to the top military command facilities.

If the early warning system (EWS) fails to inform the nation's leadership about a missile attack in time, the sanction for retaliatory strikes is prepared in response to detonations of enemy nuclear charges.

Once authorization is received, the high-level command facilities prepare launch orders. This important procedure includes a number of sequential operations that are performed together by several members of the combat watch. It is impossible for one person to perform this procedure. Once the launch commands package is prepared, it is transmitted to the troops simultaneously by all communication channels.

This operation takes a certain technologically determined minimum amount of time, which can vary depending on the limit of time "granted" to the defender by the attacker. This question of time granted will be discussed later, within the context of various nuclear retaliation options.

The main peculiarity of the nuclear C^3 system is that it must simultaneously have negative and positive controls, which are diametrically opposed to each other. In other words, it must, on the one hand, guarantee protection against an accidental or unauthorized launch of even a single missile, and, on the other hand, it should be constantly ready to transmit an order to launch, if necessary, all nuclear delivery systems.

The inner contradiction of this dual requirement is quite obvious when we take as

an example the following two extremes. First, *positive* control will be most effective if all blocking devices are removed from missiles and the C^3 system. But then there is no protection from accidents. Whereas, on the other extreme the ideal situation for *negative* control is a complete absence of missiles and nuclear warheads.

The first extreme is impermissible on principle, while we are yet to see the day when the latter is possible. Therefore, we need a golden mean between the two opposite requirements, a compromise, with all its ensuing complexities.

To sum up, one has to emphasize the rigidly centralized nature of nuclear C^3 systems. Unless the military command facility produces the guarded unblocking code value (sometimes referred to by the abbreviation *goschislo* – "state number") and the launch order itself, not a single missile with a nuclear warhead can be launched.

This means that the role of C^3 systems in nuclear force operations, and in nuclear deterrence as a whole, is to determine the final response to an attack. The probability of the national command authority (NCA) issuing release authority and launch orders determines whether even a single missile from the entire arsenal will be launched. Furthermore, the characteristics of the C^3 system also influence the magnitude of retaliatory strike. Even if the NCA issues an order, it may not reach some of the missiles because of damage to separate segments of the C^3 system as a result of a possible attack.

While C^3 plays a decisive role in nuclear deterrence (a role equal to that of the nuclear weapons themselves), there is the other side of the coin. Operation of strategic C^3 can result in a number of problems for global security, which can lead, under certain conditions, to incidents with nuclear weapons and even to a threat of nuclear war. It is necessary to analyze these problems and possible actions to reduce potential threats.

Why is it necessary to take C^3 into account in estimates of strategic stability and ways to strengthen that stability? There are six major problems that suggest the necessity of such an approach:

1. Absence of mutual accurate controls over the reliability of national systems for protection against accidental or intentional misuse of nuclear weapons. Numerous statements by national leaders about an "absolute guarantee" against unauthorized launches of ballistic missiles are hardly satisfactory;

2. Simultaneous existence of several concepts for authorized use of nuclear forces in a hypothetical conflict; the danger of a launch on warning (LOW) posture, which both Russia and the United States consider to be central to their nuclear strategy;

3. The hair-trigger state of a considerable portion of the nuclear forces, which exacerbates the dangers of a LOW posture;

4. Erosion of confidence in the survivability of the C^3 systems under com-

plicated combat conditions. This lack of confidence is gradually growing as modern countermeasures against C³ I are improving (e.g. precision conventional weapons and weapons based on new physical principles), and as a result of economic, political and social factors;

5. Growing concern regarding the adequacy of nuclear C³ systems in Pakistan, India and Israel, as well as the threshold nuclear powers;

6. Impossibility of further and deeper reductions in SNF without taking C³ into account, absence of acceptable methods for determining a reasonable balance for nuclear forces and their C³ systems, and, consequently, excessive expenditures by nuclear powers. Taking into account only the quantity and characteristics of nuclear weapons in order to estimate the level of nuclear deterrence is becoming, with further reductions in strategic arms, more and more naive.

Let us have a more detailed look at the problems mentioned.

1.2 The "Black Box" of Negative Control

Technical protections against accidental or unauthorized launches of nuclear missiles (in American terminology they are called PALs – permissive action links) that are integrated within C³ systems, as well as the whole organizational system of such protections, have always been the most secret topic in the entire range of issues related to nuclear weapons. At least, this has been the case in Russia. As for the United States, some data about American PALs have been published and discussed in the mass media but the issue remains largely undisclosed. (See more on this in Chapter 2.)

Cooperation and openness in this area between the nuclear powers would obviously be useful. Of course, public disclosure of all technical details is impossible, but a system of mutual verification between official experts and government agencies is necessary. Such a system of verification would allow national leaders to speak about a "100 percent" (or some other) guarantee, based on mutually agreeable, reliable international standards, verified in place and in action.

In principle, it is not so difficult to implement such a system as long as there is the political will to do so. There is no risk here for national security. The problems arise when it comes to national sensitivities: each side has reasons to be concerned that in the course of technical information exchange some shortcomings in its system would be revealed. Such revelations, however, are inevitable, because each system, when compared to another, has its advantages and disadvantages. But these negative consequences of openness would be more than compensated by the great benefit for both sides, and the world as a whole, that are obtained from the introduction and exchange of the best experience.

As noted, until now the United States and Russia have taken no significant practical steps toward cooperation in nuclear C^3. To be fair, though, one should mention that the United States has made some attempts concerning the issue of negative control.

Many experts believe, without official confirmation, that in the early 1960s the United States offered to equip Soviet missiles with American protections against accidental or unauthorized launch. Moscow turned down the offer from fear of losing face, and the decades since have confirmed the reliability of Soviet analogues of PALs.

In 1991, working groups of experts from the United States and the Soviet Union, headed respectively by Assistant Secretary of State for International Security Richard Bartholomew and Deputy Foreign Minster A.A. Obukhov, met for consultation about the problems of nuclear weapons.

Other participants in the meetings were V.G. Komplektov, the Soviet ambassador to the United States, Lt. Gen. F. Ladygin, the chief of the Treaty and Legal Department of the General Staff, as well as other officials. From the United States were Assistant Secretary of Defense S. Hadley, and representatives from the National Security Council, the CIA, the Joint Chiefs of Staff (Gen. J. Shalikashvili) and other agencies. Representatives of Ukraine, Belarus and Kazakhstan were also present. Cited below are some previously unpublished excerpts from the records of these meetings.[4]

> *Bartholomew*: "It has appeared to us that President Gorbachev's statement did not contain a response to one of President Bush's initiatives, that is our proposal to begin dialogue about command and control of strategic nuclear weapons."
>
> *Obukhov*: "In his TV statement, M.S. Gorbachev said that we 'are ready to enter into a substantive dialogue with the United States on developing safe and environmentally responsible technologies for storing and transporting nuclear warheads, methods for utilizing nuclear charges, and improvement of nuclear security.' The statement also said that 'in order to strengthen the reliability of control over nuclear weapons we are unifying under a single operational directorate all [SNF] and are including strategic defensive forces[5] in the same service of the armed forces.' … Thus, I think that the Soviet side gave an exhaustive response to the U.S. initiatives. At the same time, since the American side specially emphasizes the issues of nuclear C^3, we would like to hear additional ideas from your side about concrete proposals."
>
> *Bartholomew*: "The statement by President Bush mentioned, in this relation, possible measures to improve the command and control system, which could preclude unauthorized use of nuclear weapons."
>
> *Shalikashvili*: "In particular, we would like to discuss the following issues: technical measures within the existing system of command and control of strategic nuclear weapons, preventing unauthorized use of these weapons; procedures which are an

element in the strategic command and control system, preventing the possibility of an accidental or intentional launch of strategic offensive systems of different types ... I would also like to stress that the American side is not offering a detailed exchange on this subject that could touch upon subjects related to state secrets and national security interests."

Bartholomew: "In this context I would like to note that the very top of the chain of command of strategic forces in the United States is occupied by civilians, and not by the military."

Obukhov: "The Soviet Union has a system of command and control of [SNF] that ensures reliable operation of nuclear weapons and guarantees against their unauthorized use. Just as in the United States, in our country it is a civilian – the president of the Soviet Union – who is the commander in chief ... We have listened with great attention to Gen. Shalikashvili's ideas regarding possible discussions about the system of strategic C³. It is becoming clear to us that it is the issue of developing procedures providing for even more reliable guarantees against unauthorized use of nuclear weapons, but without going into the area related to the interests of national security. ... We will recommend to our leadership that these questions are reflected in the course of the future contacts with the American side. In particular, they could be touched upon during the forthcoming meeting with [Soviet] Defense Minster Ye. I. Shaposhnikov."

Bartholomew: "We will certainly follow your advice."

From the dialogue quoted above it is apparent that the Soviet side offered, diplomatically, to further clarify the matter because Moscow was not yet ready, at the political level, to agree in principle to begin concrete discussion about C³. It is also apparent that the American side was primarily interested in negative control.

A month and a half later, the sides resumed the conversation:[6]

Bartholomew: "The next important issue on our agenda is the system of command and control of nuclear forces. ... Naturally, control of nuclear weapons is in the competence of the Soviet authorities themselves. At the same time, in view of the changes unfolding in the [Soviet Union] today, the United States has an objective interest in the reliability of the Soviet nuclear arsenal's controls. The United States is in favor of keeping the nuclear weapons in the [Soviet Union] under unified collective command and control without any prejudice to the relations between the sovereign republics. ... We will inform you about the system of command and control of U.S. nuclear forces. This will be the first exchange of information of this kind."

Further on, Shalikashvili briefly presented the main principles of command and control of the U.S. strategic forces. Among other things, he said:

> "... Earlier the [Soviet Union] and the United States did not discuss these rather sensitive problems. But under the present improvement in Soviet-American relations, it is important that both sides have an idea of how the other side's nuclear C^3 system is organized. ... Of special importance in the organizational structure of the U.S. nuclear command and control system is civilian control of the armed forces as a whole and of nuclear forces in particular."

Within the framework of this initiative, the American side presented its partner with a working document entitled "The System of Nuclear Command and Control," with the expectation that after getting acquainted with it, the Soviet side would reciprocate with its own materials.

The General Staff of the Soviet Armed Forces tasked its Center for Operational and Strategic Research to draft the reciprocal materials. At that time, I worked at the center as the deputy chief of the division studying the problems of command and control for the Armed Forces, and directly participated in this work. When we were given the materials provided by Bartholomew's group, we could only smile. They contained only the most general, well-known principles of American nuclear C^3. It was clear that our partner also realized this and was just making the first small step forward, wary of scaring off its counterpart. The main emphasis in the U.S. materials was on the necessity of mutual exchange of information about protection against an unauthorized launch.

Our leaders could do nothing else but order us to prepare similar material, which we did, emphasizing the primary importance of protection against unauthorized actions within the C^3 system. Both the Soviet and U.S. materials were of no value to the opposite side, but their exchange at a high official level created some hope for a breakthrough.

In the course of the meeting cited above, the following exchange took place:

> *Bartholomew*: "I propose establishing a working group to discuss the issue of the nuclear forces command and control system. ... We would like to receive information about the Soviet system of nuclear forces C^3. For instance, we would like to know who in the [Soviet Union] is authorized to order the use of nuclear weapons; how does this system operate in view of the emergence of the sovereign republics; how is the collective and simultaneously centralized control implemented, etc."
>
> *Obukhov*: "The issue of nuclear C^3 really is extremely important for our nations, as well as for the whole world. We understand U.S. concerns about these matters in view of the changes happening in our country. I would like to direct your attention to assurances, given by the [Soviet] president during his meeting with George Bush

> in Madrid, that command and control of nuclear weapons in the [Soviet Union] is 100 percent reliable. There is no possibility of unauthorized use. In his interview with the American magazine *U.S. News & World Report*, the president of the [Soviet Union] stressed that there is no danger of weakening in nuclear command and control. He said: 'If there are any discussions, they concern only the structure of the Armed Forces and the degree of change in the role of the republics, so that they could have a greater say in the formation and command of the Armed Forces.' ... We have already discussed these questions during consultations in Moscow in October of this year, and asked the American side for a number of clarifications. The comments that we've heard today do clarify what aspects the U.S. side would like to discuss. Subsequent discussions will help to make things even clearer. ... Our side will be represented in the experts' working group by F.I. Ladygin and S.A. Zelentsov."

When Gorbachev spoke about "100 percent" reliability of command and control systems, this absolute (maximum) value, while not a clear-cut technical parameter, was supposed to reassure Americans. They could expect that the Russians would share such a brilliant achievement with them, especially since the decision was actually made to report to the leaders of both nations on the need to begin work involving C^3 experts.

But as far as I know, these exchanges had no sequel. Even if something has been done in this area, there have been no official announcements about it. It would be surprising if the public were not informed about bilateral efforts to prevent accidents with nuclear weapons. If such contacts are taking place at all, they should be announced.

Today there are no direct indications of any immediate threat to protection of nuclear C^3 against unauthorized actions. I worked for many years on Soviet and Russian C^3, and can confirm that the reliability of the blocking devices is sufficiently high. American experts generally are also certain about the protection of their C^3 system. Thus, Gen. Bernnie Davis at Strategic Air Command's headquarters said: "As far as the United States is concerned, it is impossible to accidentally launch a nuclear weapon. Impossible. Just not humanly possible – or not machine possible – for an accidental launch. And for the Soviets, I'm very confident they have similar safeguards."[7]

However sincere, this is only the personal opinion of an expert, and not a reality verified and confirmed by both sides. There are continuing doubts about the robustness of negative control.

For instance, there is the recurring issue of U.S. SSBNs, which carry on board all the necessary documents and means for autonomous launches of SLBMs without NCA authorization. In particular, during the consultations described earlier, Sergei Rogov, director of the Institute for the Study of the USA and Canada, asked, among other questions, "if there are any plans to install blocking devices on U.S. SSBNs." American sources have noted some incidents with blocking devices in the United States: "...[T]he upgrade of safeguards on the weapons will not solve the problem of safeguarding the codes themselves, a point driven home by a December 1994 incident in

which the extant unlock codes for strategic forces were compromised aboard a U.S. Strategic Command airborne command center."[8]

Another problem of the same kind is the technical possibility of delegating missile launch authority down from the NCA to lower levels. It is impossible, in principle, to avoid such a scenario within the C^3 systems of the nuclear powers, but how and under what circumstances it could be implemented is a very complicated question. The absence of an agreed-upon approach can also result in losing control over nuclear weapons. Until now it has not been said openly, at least not in Russia, who really can give the order to launch strategic missiles – the president, minister of defense, General Staff or someone else? How many options are there and which one is the primary option? This is not idle curiosity given the political events in Russia during the last 10 to 15 years. It is the heart of negative control and the public should be completely aware of it. The same applies to other nuclear powers.

For five years (1994-1999), Russian and American SNF took part in a successful program named Shadow. Under this program, Russian and American missile officers learned about the conditions of service of their opposite numbers, and sometimes even played their opposite numbers' roles. Regarding this, Col. Gen. Vladimir Yakovlev, then the SRF commander in chief, said:

> "The greatest fear in the United States regarding the Russian strategic forces is that our systems might not be reliable enough, which might lead to an unauthorized launch. The Shadow program proved the opposite ... Gen. [Eugene] Habiger even told me we are resolving these issues even better that the United States. I visited the launch control centers of a regiment and a brigade and looked into these issues in the United States, and I can state responsibly that our systems providing for safety and transmission of combat commands are not any worse, and in some cases are even better than the American ones."[9]

Apparently, the former commander in chief was right. Still, this is only an interview, not an official document of a joint U.S.-Russian expert evaluation. One of the main reasons for Western concern about the reliability of Russian negative control is the widely-held opinion that many elements of the Russian C^3 system are physically obsolete. Russian officials do not deny this: "The majority of stationary command posts and 60 to 70 percent of the C^3 equipment of the troops and weapons of the strategic weapons are past their service life. ... The situation is not any better in the Space Defense Troops, where more than 60 percent of the information systems are past their warranted service life."[10]

Despite the reassurances of the SRF's former commander in chief that the negative control of the Russian C^3 system continues to be very safe, one cannot completely exclude a certain vulnerability to its safety due to aging.

It is difficult without detailed knowledge of the real situation to speak about complete protection against unauthorized actions in all the nuclear powers today, and more so in the future under different domestic and international situations. The growth of terrorism and improvements in technologies available to terrorists are a legitimate source of concern. At the very least, there is no alternative to an exchange of the best experience in this field, and mutual help among the members of the nuclear club that is not limited to consultations, but could perhaps include technical and financial aid.

Probably, protection against accidental or unauthorized launches of nuclear missiles is not only a national problem, but more of an international one. The danger is in the complete lack of knowledge of the situation amongst the nuclear powers.

1.3 Should We Trust the Display?

Information on PALs is classified, but it is easy to prove that cooperation is necessary. On the other hand, quite a lot has been published about other aspects of C^3. Thus, for instance, much has been said and written about the use of nuclear weapons. (See Chapter 2 and elsewhere.) Some explanations are in order, however, for readers who are not experts in this subject.

The official operational scenarios of pre-emptive strikes against a potential enemy are distant history now. In the 1960s, for instance, the list of commands for the Soviet C^3 system included an order to "launch at designated time ... ." In essence, it was an order for a pre-emptive strike. But as Soviet-American contacts developed, some time in the early 1970s, this directive gradually disappeared from combat orders at command facilities, and then from screens of command and control equipment altogether. Of course, it is impossible to completely exclude the capability for a first nuclear strike either theoretically or practically. But the Russian General Staff's current operational plans do not have such an order. Nuclear weapons can be used only in response.

But in response precisely to *what*? NATO's expansion to the East, the 1999 war against Yugoslavia, and the weakening of Russia's conventional forces have all raised discussions in Moscow of revising the official position in this matter. The first revision had been made in the new military doctrine adopted in November 1993, in which Russia renounced its earlier pledge of no first use of nuclear weapons. The Concept of Russian National Security adopted in December 1997, stated that nuclear weapons could be used "if there is a threat to the existence itself of the Russian Federation as a sovereign state." Once Vladimir Putin came to power in Moscow, more precise formulations were urgently added. In the Concept of National Security of the Russian Federation, signed by the acting president in his executive order No. 24 of Jan. 10, 2000, Russia declares the principle of using "all the weapons at her disposal, including nuclear weapons, in order to repel an armed aggression, if all other means for resolving the crisis situation have been exhausted or have proved to be not effective."[11]

It is apparent that the nuclear threshold has been lowered even further. Two factors, however, are worth mentioning. First, from the technical point of view, all of this

changes nothing in the C^3 operational capabilities of the Russian SNF. No one will reintroduce into it the "launch at designated time" as an anachronism. The new concept could be implemented through the existing system simply by transmitting a launch order at the appropriate moment. Second, one should take into consideration the psychological aspect of this problem. Even when the Soviet Union and Russia pledged no first use, no potential aggressor could count firmly on this pledge. No matter what, a would-be attacker had to take into account that in a critical situation Russia, or the Soviet Union, would use the means of last resort to protect itself. So, such declarations are not worth much in the military sense.

Ideas on the possibility of a limited, "regulated" nuclear war, occasionally revived in the West, are also not viable. Long ago, Georgi Arbatov wrote: "The idea itself of introducing 'rules of the game' and of artificial limitations 'by agreement' is based on an illusion and is without foundation. It is hard to imagine that nuclear war, if launched, could be held within the framework of the 'rules' and not grow into general war."[12]

Daniel Ford writes: "The gap between the strategy of controlled escalation and the command and control system's present capability is [in the words of Paul Bracken] as far as from here to the planet Uranus."[13]

These statements continue to be true today.

Today, however, ideas criticized by Arbatov and Ford appear not only in U.S. sources, but in Russian military literature as well. Thus, two Strategic Rocket Forces (SRF) generals, N. Ye. Solovtsov and V.T. Nosov, stated in November 1994: "The mission of deterrence advances an additional requirement to the [SNF] – an ability to deliver selective, even single, nuclear strikes to a wide range of distances, with minimal environmental consequences."[14]

It is difficult to determine whether this opinion was a reflection of Russian official positions. In any case, it may be explained by the fact that Russian (as well as any other) C^3 has the technical capability to launch a strike, including single launches, against any number of targets. The authors cited above, as specialists, were most probably talking about the development of this "technical capability" in a command and control system in order to increase its flexibility under complicated circumstances of a retaliatory strike. Using such a capability, however, for advanced planning of a limited nuclear war would be a completely different matter. It is a prerogative of politicians. Unfortunately, under the cover of the new military doctrine, the support is growing in Moscow for allowing limited nuclear strikes in response to an attack, and this support is in direct proportion to outside pressure against Russia. However, it is always stressed that the goal of such strikes is not "complete destruction of the aggressor" (as they used to say in the Soviet days), but rather stopping the war before it becomes a global catastrophe. Obviously, this "reassurance" does not improve matters, as a "limited" nuclear war is a utopia. One can only hope that this Russian position is only a warning to a potential attacker, the means to preserve peace.

For a long period, until recently, Russia and the United States have generally be-

lieved that reliable mutual deterrence could be provided by developing nuclear weapons and C^3 systems based on a strike in response to early warning, called launch on warning (LOW), as well as in response to an actually delivered strike (launch under attack, or LUA). Combining these two approaches could have been possible if it did not create a number of serious problems in technology, economy and strategy. For now, let us look at strategy.

The strategic aspect of the problem asks which responsive action should be the dominant one, i.e., how should the NCA act at the moment of nuclear crisis? Also, can LOW and LUA exist separately, i.e., can they exclude one another?

From the standpoint of strategic stability, it is unacceptable to follow only a LOW concept. One cannot drive the leaders of a nuclear power into a corner by making them react impulsively and immediately to early warning information without the right to make a mistake, without the insurance of the LUA concept, which provides for retaliation under any circumstances.

Alexei Arbatov writes: "The function of making the most important of all imaginable decisions by political leaders actually becomes a fiction, a monkey's conditional reflex: the light turns on – the monkey pulls a handle – a banana appears."[15] Further, he makes a very sharp and bold – but absolutely correct – conclusion:

> "There is no doubt that after the end of the Cold War, even under conditions of possible future great international tensions, risk of a nuclear disaster because of an accident is much higher and more terrible than the risk that in case of a hypothetical attack against Russia her retaliatory strike would be delayed, less destructive or even won't take place at all. Since the danger of war has been reduced, the last word should belong to politicians: the strategy of delayed second strike appears to be the only reasonable approach."[16]

The subsequent logical question is: if C^3 within the framework of LUA guarantees retaliation against an attacker reliably enough, why incur additional expense for LOW?

Such questions are numerous, and they will be considered in the following chapters. For now, let us note that today there is no satisfactory explanation for an NCA's actions in a unique crisis situation, which one hopes will never occur.

Russia lacks an official unclassified document regulating the actions of political leaders in case of a nuclear conflict. A good example of this shortcoming is the notorious case in which the Russian EWS "detected" in early 1995, the launch of a Norwegian meteorological rocket. Leaving aside Russian leaders' political use of this action (detection), let us ask a simple question: how should then President Boris Yeltsin and the General Staff have acted if that rocket had been flying (even by mistake) toward Russian territory?

As Yeltsin confessed, he "used the nuclear briefcase for the first time" on that occa-

sion. The whole episode smacked of a poor joke and made many specialists in the Ministry of Defense and the defense industry wince. The president demonstrated very vague knowledge of the subject. This came as no surprise, because Russian political leaders (just as their Soviet predecessors) never conducted any serious training for such a case. Under such circumstances, it makes no sense whatsoever to speak about use of nuclear weapons, since it is the president who is supposed to be one of the main actors in such a case.

For the sake of comparative analysis, let us refer to some examples from the American experience:

> "[A]s Richard DeLauer, the under Secretary of defense for research and engineering, has noted, the civilian officials' preparation for their roles is less than impressive. 'One of the things we have discussed over the years is the difficulty of getting the president even to sit down to practice,' he said. 'I guess President Carter was the first president ever to visit the National Command Post and sit down where he was supposed to sit and at least be briefed on what it all means. President Nixon never did, Johnson never did, and some of the security advisers, like Kissinger, never went down there.' ... A former Pentagon official said that Richard Nixon was 'the great neglector' of this subject while Jimmy Carter 'had an almost morbid' interest in it and spent considerable time trying to master the intricacies of the [Single Integrated Operational Plan]. Carter volunteered to sit down with his successor to discuss the subject, but his offer was rebuffed by President Reagan."[17]

Under LOW, the NCA has very little time for decision-making. Under the best circumstances, in Russia it would be not more than two or three minutes. This is if the Russian EWS, the capabilities of which have been considerably reduced, functions normally. Theoretically, a nuclear response will take place if the NCA has such authority from the Russian people and an agreement from the members of the Commonwealth of Independent States.[18] And, of course, if the president will take upon himself the ultimate responsibility for action in a complicated, confusing situation, having as his only justification the information on EWS screens about the (possible) beginning of a (possible) nuclear attack against (perhaps) Russia. (But, as President John F. Kennedy once said, "later there will be no one left to judge.")

This is, approximately, the argument of LOW opponents in Moscow. The supporters of LOW answer as follows: If one has to wait for a nuclear strike against one's territory to actually take place, it may turn out that there is nothing left to launch, that the order cannot be transmitted because the communication system is wrecked, and that the NCA will be unable to make a decision because it has perished by that time. Supporters of LOW stress that in their scenario any retaliatory strike will be weak and its probability will be low.

Such arguments may seem a bit academic, but theoretical concepts on the use of nuclear weapons are backed up by concrete and expensive C^3 systems. In the case of LOW, the system is not highly survivable, but rather a fast and all-seeing effective EWS with a mostly stationary system of command posts linked together by cable and satellite communication channels. Add to this a "decisive" president. The concept of LUA, on the contrary, presupposes a relatively slow C^3 system that is highly survivable under the most adverse conditions. This is the network of mobile and super-hardened command posts linked together by special highly survivable channels of command and control. (Literature about one of these command posts is available.)[19] Add to this a cautious NCA, which has, thanks to a system like this, the right to make a mistake (i.e., the right not to be in a hurry).

Until the disintegration of the Soviet Union, its C^3 system was built on the principle of LOW; as Arbatov said, "... the one-sided Soviet strategy ... relied excessively on the launch-on-warning principle."[20]

Now this system looks less impressive. As for LUA, today technical support for its implementation is insufficient in both the United States and Russia. In which direction will nuclear postures, now subject to reductions, develop? Supporters of LOW maintain that the drastic cuts in nuclear arsenals require a reliance only on LOW, since after the years 2007-2008, according to their calculations, there will be no missiles left for a retaliatory strike after absorbing an enemy attack. Supporters of the delayed second strike (DSS) are pointing out that today negative control is much more important than positive control, and that the notions of "few" and "many" regarding nuclear retaliation are quite relative.

The arguments continue, but in practice both sides manage to obtain funding for their main technical programs. A good deal of money is being spent while there is still no strategic clarity. Combat documents at the nuclear command facilities continue to reflect both types of scenarios, and they are periodically gamed at command and staff exercises. Notably, this confrontation has been somewhat muted in recent years. Various scenarios of limited nuclear conflicts with an abstract potential enemy have complemented the two existing scenarios. (See more in Chapter 2.) However, these scenarios are not likely to have a significant impact on the main direction of military-technical policy in Russia and the United States regarding nuclear C^3. In Russia, with its current economic problems, not only the political opposition but also clear-sighted members of parliament are raising the issue of logical, open substantiation of strategic concepts, to allow for more optimal defense planning.

1.4 The Hair Trigger

Strategic stability is seriously threatened by the exceptionally high technical readiness of nuclear forces, and of their C^3 system, for immediate action. The time from the decision to the launch is now only several minutes.

It sounds like a paradox. For three decades, both nuclear superpowers have empha-

sized the combat readiness of their nuclear forces above anything else, squeezing minutes and seconds out of technology. In the Soviet SRF, combat readiness was absolutely above all other requirements, and was supposed to be perfected constantly. I have also taken an active part in this effort. Now, however, combat readiness has become an obstacle.

The paradox, nonetheless, only seems to be true. Everything depends on one's vantage point. From the military point of view, high combat readiness of any weapon is necessary. Along with the destructive potential of nuclear charges, it determines effectiveness of deterrence. A different picture emerges from a political vantage point, which takes global security into account.

It is politics and ideology that determine the characteristics of nuclear C^3 systems. Because the United States and the Soviet Union relied for a long time on mutual deterrence, today we have the technical capability to respond immediately and transmit the launch order to the missiles within 10 to 15 seconds. However, if it is officially acknowledged that global security has the top priority, that presidents have the right to make a mistake, that they have *no right* to authorize a retaliatory strike only on the basis of information from an EWS (even the most reliable one), then a different posture becomes possible, which no longer emphasizes speed of response above all else.

Combat readiness, understood broadly, involves not only the capacity to notice a threat in time, evaluate it and rapidly transmit the order to respond. It has another aspect: survivability of nuclear forces and their C^3 system under the most adverse conditions. To develop such a capability is tantamount to relying on the LUA concept, using technology to provide for the right to make a mistake.

The idea of lowering the readiness of nuclear forces is becoming increasingly popular. Along with studying the possibility of a transition, through changes in the C^3 systems, from LOW to a less dangerous concept of DSS, some direct measures such as delaying the preparation and launch of missiles in case of unexpected accidents are either being studied or implemented. In the United States and Russia, some missile launchers and elements of the C^3 systems are being taken off combat watch, nuclear warheads have been removed from the missiles, etc. The idea of deep reductions, down to days, weeks and months, of the readiness of all nuclear force components (weapons, C^3, etc.) – "zero alert" – is described in detail by Dr. Bruce G. Blair.[21] In the following chapters, I will analyze this aspect of his work. The idea of zero alert is worthy of a most attentive study.

Even if nuclear readiness is reduced to a very low level, in the case of a political confrontation, the two sides may begin to upgrade readiness. This process of upgrading "back" is dangerous by itself: one side can find itself ahead of the other and try to use this "advantage." In such circumstances, one needs something beyond political efforts (which we do not consider in this study) capable of preventing a conflict from turning into a catastrophe. At the conceptual level, it is the LUA strategy which can guarantee retaliation. At the level of technology, we may think of some measures within the C^3 systems themselves. (See more in Chapter 6.)

Today, in any case, it makes no sense to keep the still huge nuclear forces and their C^3 systems in a dangerous hair-trigger state.

1.5 The Illusion of Weakness

Concerns over the possible weakening of nuclear C^3 systems can result from, first, the continuing development of different means of attack, and, second, because of internal problems in nuclear states.

The effectiveness of intelligence collection against operation and modernization of nuclear C^3 systems is increasing. Means for disrupting C^3 systems are being improved. Primarily, these are munitions with deep underground impact, strike anti-satellite systems, Stealth aircraft, electronic warfare systems, and promising weapons based on new physical principles, especially super-electro-magnetic pulse (EMP) weapons. In *Global Zero Alert for Nuclear Forces*, Blair speaks about "the bane of Russian planning":

> "The Trident D-5 force alone, representing only 18 percent of the active U.S. strategic nuclear stockpile (1,344 of our 7,700 warheads), poses a qualitatively new threat to Russia. The missile's pinpoint accuracy means that practically any target in Russia except a handful of underground command bunkers is vulnerable to destruction by U.S. SLBMs, even though most D-5s carry warheads with relatively low explosive power. ... If directly targeted, critical facilities in the nuclear command system in the Moscow area would stand little chance of surviving."[22]

It is difficult to judge *a priori* how small the chances are for command facilities to survive accurate strikes by Trident D-5 SLBMs, but it is obvious that they present a serious threat to the Russian C^3 system. They, as well as other means of attack, threaten the military C^3 systems of other countries, such as China, at least as seriously. And this is disturbing.

A Russian expert, stressing the continuous improvement of counter-C^3 measures, writes (with reference to a U.S. source):[23] "... It is no accident that American experts believe that under conditions of deep reductions and given the qualitative composition of strategic nuclear forces, 'resistance to the temptation for a first strike in relations between Russia and the United States will be the weakest since the early 1970s.'"[24]

It is self-evident that a strong, highly survivable system of nuclear C^3 is a stabilizing factor, and can never become destabilizing. Indeed, the attacker in a nuclear conflict can have a weak C^3 system, since a highly survivable one is not necessary for a first strike. But a weak C^3 system may, under certain circumstances in a difficult situation, provoke the opposing side to carry out a first strike to decapitate the opponent's nuclear forces and thus prevent his retaliation or his first strike. Of course, such scenarios are not in the spirit of today's relations between nuclear powers, but the very nature of the nuclear world makes it necessary to take all possible scenarios into account.

The disintegration of the Soviet Union has awakened serious concerns over the state of its nuclear C^3 system. The breakup resulted in serious, although not decisive, changes in the Russian nuclear C^3, as well as in control over nuclear weapons located in Ukraine, Kazakhstan and Belarus. The first, and most important, factor was that Russia had to exclude those nuclear forces not deployed on its territory from the combat organization of its SNF. This was done because Russia actually lost not only administrative, but also operational, control over these forces. The second important factor was the destruction of the single EWS. The majority of the early warning radars being operated, modernized or brought on line by the Soviet Union turned out to be outside of Russia: Skrunda in Latvia, Nikolaev (Sevastopol) and Beregovo (Mukachevo) in Ukraine, Mingechaur (Lyaki) in Azerbaijan, Balkhash in Kazakhstan and Gantsevichi (Baranovichi) in Belarus. Thus, out of nine deployed Soviet EWS radar regions, only three have remained in Russia: Olenegorsk (Murmansk), Mishelevka (Irkutsk), and Pechora.[25] Although the Russian government has concluded agreements with some of the former republics about their operation, the Russian military leadership cannot fully rely on these radars in its strategic planning. A good example is the elimination of the radar in Skrunda. The significance of this loss is clear: without reliable "eyes" in the SNF C^3 system, it is difficult to argue in favor of a LOW posture, with all the logical consequences.

Furthermore, the disintegration of the Soviet Union resulted in the collapse of the huge research-industrial cooperative network, which produced not only strategic rockets, but also C^3 equipment (Chapter 4 will list the design bureaus and factories that Russia lost). Although Russia has rebuilt this cooperative network using its own resources, it will have difficulties in developing its C^3 system for years to come. Significant cuts in the defense budget will have a similar effect.

The former chief of the Main Operational Directorate of the General Staff, Col. Gen. V.M. Baryn'kin, said in 1996:

> "The disintegration of the [Soviet Union] has considerably complicated working conditions for the military command and control system. The best elements of this system, with some exceptions, have been left outside of Russia, while what remains in Russia, naturally, cannot fully provide for the needs of command and control. Besides this, in recent years, because of the general economic decline in the country and disruption of the scientific and production links between the [Commonwealth of Independent States] countries, the tempo of development of the command and control system, including the communication system, has been sharply reduced ... Changes in the country's economic situation have resulted in a failure to finance work for the maintenance of readiness and further development of the command and control system at any more than 40 to 50 percent below the required level. As a result, by the year 2000, the cycle to introduce new command and control equipment will be more than 60 years, and the whole process will no longer be realistic."[26]

Of course, it is too early to talk about a 60-year-long cycle of developing new command and control systems for the SNF, but the situation has not improved since 1996. The Russian defense industry was particularly hard hit by the budget crisis of spring 1998 and by the subsequent financial crash of Aug. 17, 1998. According to Arbatov,

> "In the spring of 1998, the planned defense expenditures were first cut by the Sergei Kiriyenko Cabinet from 82 down to 61 billion rubles, and after the Aug. 17 crisis the financing of defense was reduced even further, and as a result by the end of that year the actual defense expenditures were only 50 percent of the planned level. By the end of 1998 the military personnel was reduced by 25 percent, while the military budget – by 50 percent. Since it was impossible to reduce proportionally the expenditures for operation and maintenance as well as for investment, the deepest cuts were made in the budget for [research and development] and design, weapons and equipment acquisition, and capital construction. They were financed only at the level of 14 percent from the plan (4 billion rubles instead of the planned 28.5 billion rubles)."[27]

Given the poor condition of the Russian economy in general, and the defense industry in particular, the programs for C^3 development were practically frozen between 1996 and 1998. If during the Soviet era the share of spending for the improvement of strategic C^3 constituted from 10 percent to 15 percent, or even 20 percent, of the total SNF spending, between 1996 and 1998 it fell down to 1 percent or 2 percent. However, in 1999 the C^3 share in the SRF returned back to 10 percent, mostly because research and development work on the Toppol-M ICBM was over and its mass production began; therefore, some redistribution of research and development funding became possible. Yakovlev, then the SRF commander in chief, said in this regard, "When working on the program for the future SRF ... a certain redistribution of resources has occurred between the development of informational and command and control systems and the strike elements of the SRF."[28] It is also possible that the Russian leaders have realized at last that C^3 could no longer be neglected and started making some steps to reverse the situation. But despite all of this, with the economy in decline and low defense budgets in absolute terms, this 10 percent will hardly be sufficient for the development of Russian C^3.

All the factors listed above may create an impression of Russia's nuclear impotence among less knowledgeable observers, or at least of a gradual deterioration in its ability to control its nuclear forces. This would be a dangerous illusion. Subsequent chapters will explain why. At this point, it is sufficient to say that neither the continuing degradation of Russian strategic C^3, nor the problems of its modernization, nor an increase of all types of negative external factors affecting it can exclude, in principle, some probability that it will work when necessary. The result will be catastrophic for anyone trying to test this

system. *The main task is not to cast doubts upon the deterring role of strategic C^3, but to study how this role evolves and to prevent dangerous uninformed speculation on the subject.*

Last, from command and control's point of view, the disintegration of the Soviet Union not only created difficulties within Russia, but also raised some new questions at the global level. Much had been recently said about the Ukraine's technical ability to take operational control of "its" ICBMs within several weeks, using the remaining C^3 elements in Vinnitsa, Khmelnitsk and Pervomaysk, as well as the research and production capabilities of the design bureaus and factories in Kharkiv, Kiev and Dniepropetrovsk. Now Ukraine has been proclaimed to be nuclear-free, but it is not ICBM-free. If this independent country, or Kazakhstan or Belarus for that matter, would plan to use its remaining missile technology, specialists and rich experience from the Soviet period, we should take into consideration that they have considerable experience in the field of command and control.

1.6 The Third Countries

There is a concern over nuclear command and control in threshold states that actually have nuclear weapons, but do not have official status as nuclear powers: Pakistan, India, Israel, and some others. In the course of the Soviet-American consultations in 1991 mentioned earlier, one of the American participants said, "the United States is concerned over the unreliability of ballistic missile C^3 systems in the threshold states ..."[29]

A Russian expert, with reference to an American source,[30] writes:

> "Some American scholars propose that their government should help create reliable systems for 'positive' and 'negative' control of nuclear weapons in the new nuclear states in order to prevent any unauthorized or accidental use. These experts refer to an example of cooperation in this field in the past: in the early 1960s the United States supposedly informed both the United Kingdom and the USSR about the design of their novelty – 'electronic locks' on nuclear warheads."[31]

It is very difficult to come up with anything definitive on this subject. Any attempts at control over the C^3I activities of third parties are going to run into their lack of official status as nuclear powers. Still, some things can be seen without their cooperation:

> "Although little is publicly known about some of its particular elements, especially the specific line of authority and other more procedural aspects, the physical elements are quite apparent. The construction of underground command-and-control centers takes at least a year and is easily noted by photographic reconnaissance satellites; communications facilities, navigation stations, and radar sites are mapped by a variety of signal intelligence (SIGINT) systems; and satellite launches and or-

> bits are continuously monitored, although the precise mission must necessarily often be inferred."[32]

Such information is not reassuring enough of the safety of these C^3 systems. Therefore, positive results are likely to be achieved only if an international solution to the main problem is found: elimination of nuclear weapons in the countries that are not officially recognized as nuclear powers.

If some of these countries strengthen their positions as nuclear powers, it will become necessary to include them in negotiations on cooperation on C^3I issues (although the word "cooperation" is perhaps not the best term to describe the situation). It is probably better to be aware of the situation in unofficial nuclear powers, and perhaps even give them aid in order to increase the security of their command and control, than completely ignore the issue and thus create the potential danger of nuclear accidents. Such is the paradoxical nature of strategic C^3.

According to experts, up to 20 nations could have nuclear weapons by the years 2008-2010, and the relations between some of them will certainly not be as stable as they are between the members of the official nuclear club. Regions suffering from long-standing conflicts will then become a reason for particular concern. Although India and Pakistan, after openly testing their nuclear weapons, assert that the situation in their region has now stabilized, there is no guarantee that under certain circumstances they would not resort to these powerful weapons. The situation could be made even worse by their weak, undeveloped systems of nuclear C^3: it may be tempting to suppress the enemy C^3, and these systems may be accident-prone. A nuclear conflict between these two nations could have negative impact on other troubled regions. The Middle East comes to mind first, where Israel already has nuclear weapons, and some of its perennial Arab enemies could acquire such weapons within the next few years. One may add that such nuclear nations as India, Pakistan and Israel, as well as Egypt, Libya, Iran and some other states, can develop and build ballistic missiles.

The issue of third countries has another aspect as well. They may present a threat to the command and control systems of nuclear powers. As Blair notes,

> "A related function, which is an increasingly important priority, is to monitor the launch activities of threshold states that are developing or deploying ballistic missiles. This proliferation has a growing potential to directly threaten the nuclear superpowers as well as to strain their early warning systems. It might increase the risks of false alarms and thus aggravate the problem of nuclear inadvertence."[33]

1.7 Reducing Strategic Arms Blindfolded

This section deals with accounting for command and control in estimates of strategic stability, deterrence, etc. While all the issues dealt with earlier belonged to the

dangers related to operating nuclear C^3 systems, this particular question can be described as a *problem*.

Mutual nuclear deterrence has been, and will continue to be, the cornerstone of strategic stability as long as nuclear weapons exist. One may only agree with the school of thought maintaining that nuclear deterrence is much more reliable than a conventional one. Of course, this is no reason for celebration, and the preservation of the nuclear monster cannot be a goal for its own sake. Still, it would be reasonable to view reliable mutual nuclear deterrence as the natural inevitable result of nuclear weapons' existence.

In the course of their nuclear confrontation, the Soviet Union and the United States strove for parity, which they understood as, simply put, an approximate equality of general quantitative levels of nuclear arsenals. This is so: both sides had 10,000 to 12,000 strategic warheads and 15,000 to 20,000 tactical nuclear warheads. The same principle has been adhered to since the beginning of arms reduction process: according to START I, each side is to keep 6,000 strategic nuclear warheads, while the never-to-be-implemented START II allows each side 3,000 to 3,500 warheads. This rather simplistic approach was justified by the huge absolute size of the strategic arsenals, which guaranteed destruction of the enemy and of world civilization many times over.

The process of U.S.-Russian strategic arms reductions is continuing, despite some snags, and it is becoming clear that in the near future we will have to determine why we require the level of strategic forces that we have now, as opposed to a higher or a lower one. If the level is higher than reasonable, this means excessive expenditures; if it is lower, national security is threatened. Also, why should we cling to the outdated concept of parity? Given the weakness of Russia's economy, it cannot pursue nuclear parity with the United States. Here is one of the most pessimistic scenarios, presented by Arbatov:

> "By the year 2008 ... Russia's SNF would have 600 to 700 warheads, mostly on delivery vehicles no longer adequate for reliable deterrence. Even if the United States go down to 3,500 warheads within the START II framework, they will 'unwillingly' have a five- to six-fold superiority over Russia, and if one counts nuclear arsenals of the whole NATO, the superiority will be seven- to eight-fold, the same as it was during the Cuban missile crisis."[34]

Russian experts have proposed various plans to prevent a large strategic nuclear inequality between Russia and the United States, but all these plans would result in hurting the other branches of the military, the economy, the government's social programs, etc. Of course, the SNF must remain the main priority in Russia's defense policy, and measures necessary to keep it that way will be taken, but it remains a fact: an asymmetry of nuclear potential between Russia and the United States is inevitable in the im-

mediate future. What else could be expected if Russia's defense budget is not more than 6 to 7 percent of the U.S. military budget?

When the formula of strategic balance no longer has the equality in which Russia's military analysts seek their salvation, we will have to think about new ways of estimating effectiveness of deterrence. I believe that the simple comparison of strategic arsenals is dead, and that we have to estimate the forecast final result of nuclear retaliatory strikes. The estimates of such forecasts should be performed not only by experts, but also involve a broad public participation. The C^3 factor in nuclear deterrence will play an important role in this new approach.

The command and control factor has a direct impact on the stabilizing, or destabilizing, character of different types of nuclear weapons. The dependence of a weapon's effectiveness upon the reliability of C^3 must be taken into consideration when concluding and implementing treaties on the reduction of strategic weapons.

This can be best demonstrated by the example of sea-based components of the nuclear triad. According to START II, this component could have become very important in the Russian SNF after 2003, but it is no secret that today the survivability of the SSBNs' C^3 system is low. Land-based extremely low frequency (ELF) transmitters, which are practically the only means for communicating orders to deeply submerged submarines, are relatively vulnerable not only to nuclear, but to conventional, weapons as well. This situation is a result of the Soviet Union's (and Russia's) one-sided preference for the LOW concept. Had START II been implemented, it would have been necessary to undertake drastic measures to strengthen the reliability of SSBN C^3 systems, in coordination with the tempo of reductions in strategic weapons. If this is not done, the other side would acquire an opportunity to "disconnect" the main Russian means for a retaliatory strike, and this would become a powerful destabilizing factor. By comparison, the United States has a sufficiently powerful and reliable C^3 system for its sea-based nuclear forces, which includes a global network of land-based transmitters, a group of Take Charge and Move Out (TACAMO) airborne relay transmitters, and communication satellites. Such a degree of attention to C^3 for SSBNs adequately reflects American ideas about the importance of SSBNs as the main means of retaliation.

The mutual relationship between weapons and command and control can be traced in other components of the triad. Thus, the destabilizing character of silo-based ICBMs with multiple, independently targeted re-entry vehicles (MIRVs) is further aggravated by the fact that in Russia these weapon systems have the best and fastest C^3 system. An order from the center can be transmitted to such missiles in less than a minute. At the same time, the C^3 system for the mobile ICBMs of the SRF has quite a few problems although it is more reliable than that of the SSBNs. Since land-based mobile ICBMs will play an important role in providing for a retaliatory strike, their C^3 system should also be improved.

As for strategic bombers, the task of reliably transmitting orders to them remains quite complicated, especially when they are far away from land-based UHF transmit-

ters and under conditions of high interference. Given Russia's current economic difficulties, one cannot expect radical improvements in this respect. Therefore, precisely because of C^3 problems, the airborne component of the triad has a rather destabilizing character, and it would be quite logical to eliminate it, changing the posture to a nuclear dyad.

In general, the stabilizing influence of a C^3 system is manifested in the following way: The more reliable a C^3 system is, the more weight it carries of the total nuclear potential that survives a first-strike attack, and thus can be used for a retaliatory strike. There is an economically rational prospect of developing the C^3 system in such a way as to allow the surviving strategic forces to approach 100 percent reliability, and thus create conditions for deep reductions in SNF. In this regard, it is worthwhile to pay attention to the idea of mutual limitations on further development and production of the means for disrupting C^3 systems.

The Russian and American experiences show that expenditures for C^3I and nuclear weapons as such are in the same category. This becomes quite evident if one takes into consideration the needs for research and development financing, testing, mass production and multi-year operation and maintenance of all elements of a C^3 system: a group of land-based (stationary and mobile) command facilities, and airborne and other (rail-based, sea-based) types of command facilities at all levels; automated command and control systems; networks of cable, radio, satellite, radio-relay, tropospheric and other types of communications, etc.; not to mention the expenditures for the staff of these facilities. During some periods of the Cold War, the United States and Soviet Union spent about 15 to 20 percent of all their nuclear forces' budgets on C^3 systems. (See more in Chapter 4.) So, the economic aspect of the C^3I problem is also quite important.

Two questions are in order here. First, if two concepts – LOW and LUA – coexist today, and complement each other strategically, is it possible to save money through an optimal redistribution of expenditures between them within the framework of C^3I as a whole? Second, is it possible to reduce general expenditures on nuclear deterrence by a more rational distribution of allocations to the weapons themselves and their C^3 systems? Yakovlev, then SRF's commander in chief, addressed this issue in 1998:

> "But does [Russia] need such a number of warheads if the members of the nuclear club, not counting the United States, [and Russia] have about 1,000 warheads between them? Can the government provide such funding today? And what would be the funding priority: the warheads or C^3 systems? What would make greater contribution to combat effectiveness?"[35]

Unfortunately, until now most estimates of effectiveness have been performed separately for weapons and for C^3I – both in the Soviet Union and Russia, and, to the best of

my knowledge, in the United States. Moreover, estimates of C^3 systems proper are performed either within the framework of LOW without any reference to LUA, or conversely, for LUA without any reference to LOW. This results in excessively high expenditures. Today, there are generally accepted indices and criteria taking into account the respective contributions of weapons and C^3 elements to the deterrence factor in various scenarios of nuclear conflict. If such a common denominator can be found, a better economy of resources for operation and development of C^3I and nuclear forces as a whole can be achieved.

I believe that the absence of open, convincing proof of the sufficient level of nuclear deterrence and of the corresponding structure of the nuclear forces and their C^3 system were the main reasons for Russia's multi-year procrastination over the ratification of START II. The supporters of START II during all those years had no effective instrument that could help them overcome the resistance of pseudo-patriots, who simply used START II for their opportunistic political goals.

This problem is mentioned in an interesting book about Russian nuclear weapons, but its author's logic seems to be a bit strange: "When signing all the international agreements on limitations and reductions of strategic offensive weapons, the C^3 systems always remained outside the framework of these agreements. Arms reductions do not involve C^3 systems. The C^3 system is the cornerstone of combat ability of Russia's SNF."[36]

According to this logic, since the C^3 system is the cornerstone of the SNF combat ability, it should not be taken into consideration when estimating this same combat ability for the purpose of arms reductions. But the opposite should be true. Until now, C^3 was not taken into consideration because of the monstrously high levels of nuclear arsenals and a lack of methodology for such estimates. The sides to the arms reductions process have not yet learned how to estimate together nuclear parity not on the basis of a primitive equality of initial arsenals, but by forecasting results of a hypothetical conflict. One cannot leave the C^3 factor out when estimating the final outcome of a nuclear exchange.

There is no doubt that the problems listed above, as well as other potential problems related to nuclear C^3, are serious. The issue is: how to reduce their negative impact on strategic stability? The special character of this problem, resulting from the global nature of the nuclear threat, is that it can be solved only through the combined efforts of different nations, first of all the nuclear powers. It is necessary to agree on the main principles of conduct in this area, and establish certain rules to the game.

This requires a certain degree of openness on the issues of nuclear C^3. Here is the key to solving all those problems listed earlier. During the Cold War one could not even think about such mutual confidence.

In 1968, Lev Mendelevich, a prominent Soviet diplomat, said:

> "We know so much about how you make decisions. Americans are talking about this and writing about this all the time. It is more than we can swallow. But you

> know little of how we make decisions and we are not going to tell you. Because we do know, we have some chance of influencing your decisions. Because you don't know, your chances of influencing ours are limited and we intend to keep it that way."[37]

This is a classic example of the Soviet official thinking of the time. But it is no longer 1968, and the nuclear powers have made a number of significant steps toward each other. The next important step should be in C^3.

In order to have a degree of openness in this field, one needs firm guarantees that no irreversible damage to national security will be done. Official and unofficial experts should focus all their efforts on the search for such guarantees.

It appears rational to begin with combined preparatory research whose goals will be (a) to prove whether cooperation in C^3 is beneficial to the nuclear powers, and (b) to prove, theoretically, that national security can be guaranteed with a certain level of openness in the area of strategic C^3.

Before describing a possible methodological approach to the analysis of these two problems, it makes sense to consider the achievement of experts from different countries in solving this problem during the nuclear era.

Chapter 2

The State of Scholarhsip

2.1 General Review

Ever since the dawn of the nuclear confrontation, many experts have been intrigued by the influence of command and control on the assessment of the effectiveness of nuclear forces, mutual deterrence, strategic stability, etc. The bulk of non-classified work on the matter has been published in the West, predominantly in the United States.

Issues discussed in this book have been dealt with in the works of Raymond L. Garthoff, Scott D. Sagan, Richard L. Garwin, Desmond Ball, Peter Douglas Feaver and Richard Ned Lebow, Paul Bracken, Frank von Hippel, Harold Feiveson, Daniel F. Ford, Thomas C. Reed, Peter V. Pry, John Erickson, Daniel Goure, Sherman Frankel and G. Jacobs. Scholars from the Brookings Institution – Bruce G. Blair, John D. Steinbruner, Charles A. Zraket, Ashton B. Carter and Richard K. Betts – have made a major contribution to the theory of nuclear command and control within the framework of global security.

Due to well-known reasons, there were no unclassified publications on C^3 in the Soviet Union during the Cold War. All the research was classified and only for "internal use," i.e. only within the framework of the specialized institutions inside the military industrial complex. The Soviet C^3 community, however, showed great interest in the translations of some popular Western sources. Two of the works that were translated into Russian are worth mentioning here: *Analysis for Military Decisions* – a collection of lectures delivered by the leading experts of the RAND Corporation for the management of the U.S. Defense Department and American private industry, edited by E. Quade, published in the Soviet Union in 1969, and Ford's book, *The Button*, the Russian translation of which was published in the late 1970s.

In one way or another, problems related to nuclear command and control were mentioned in many unclassified writings of Soviet and Russian scholars, but no research has been published on the specific topic discussed here. Unclassified publications on C^3 appeared in the Soviet Union only in the late 1980s. For example, it is worth mentioning here the materials published by the Kometa, a central research and production enterprise, developed under the leadership of Anatoli I. Savin, and a series of articles by the experts from the Moscow Institute of the World Economics and International Relations of the Russian Academy of Science – Alexei G. Arbatov, G. D. Lednev and others. A short book I wrote, *Otsenka Garantii* (Assessment of the Guarantee), published in 1994 by the Moscow State Institute of International Relations, may be recom-

mended as another Russian source dedicated totally to the impact of command and control systems upon the effectiveness of nuclear forces. Russian experts have examined several issues of nuclear command and control in a number of publications. *(See Appendix 1).

The majority of the mentioned works, as well as others, emphasize that the correct assessment of the effectiveness of nuclear forces is practically impossible without considering C^3. Thus, Blair, the author of one of the most definitive studies of the subject, *Strategic Command and Control: Redefining the Nuclear Threat*, says:

> "The key limiting assumptions that underlie much strategic enumeration, particularly the assumption that weapons system characteristics are the key determinants of strategic strength, require more than a cursory examination and footnote ... Command performance is quite possibly not just an important factor but the key determinant of real strategic capability."[38]

The array of questions regarding nuclear command and control considered by American experts is very broad – from general ideological, often philosophical, aspects of nuclear confrontation and mutual deterrence to detailed descriptions of specific technical systems and means; from theoretical methods of assessing the impact of C^3 to practical proposals for its further development.

American authors, such as Erickson,[39] Garthoff,[40] Goure,[41] J. Hemsley,[42] Stephen Zaloga,[43] Jacobs,[44] Blair[45] and others have written extensively on the Soviet (later Russian) C^3 system and as a whole have a high opinion of its potential:

> "The conventional wisdom in the West makes some contentious judgments about the institutional structure and style of Soviet weapon acquisition. It holds that effective procurement in the Soviet Union is handicapped by excessively centralized procedures implemented by an unimaginative bureaucracy. It holds that the Soviet approach to weapons design is conservative and produces low-quality systems (by U.S. standards). These are dubious assertions, and Western policymakers are ill advised to accept them. Most Soviet systems are not inferior to U.S. equipment. Where it matters – on the battlefield – they can be expected to perform at least as well as, and probably better than, U.S. hardware. ... This is tactical, not technical quality. ... Would more respectful attention to the Soviet system and its style not be worthwhile?"[46]

Ball states, "it would probably not be possible to isolate the Soviet NCA completely from the strategic forces or completely impair the Soviet intelligence flow."[47] Probably with such assessments in mind, former secretary of the Navy, J. Williams Middendorf, stated, "the Soviets have the best command-and-control one can imagine."[48]

There are also opposite opinions of Russian C³. Some American experts emphasize inferiority of certain technical aspects, insufficient development of satellite communication systems, conceptual inflexibility and the highest degree of centralization. The latter may be viewed as both an asset and a fault; and it will be discussed later.

As for American C³, it is described in sufficient detail in the work of Blair, Bracken, Ford, Pry, Lebow and Sagan.[49] The works by Ball and Reed can be recommended for their familiarization with the principles and practices of U.S. C³ planning (the single integrated operational plan).[50] For learning about American means of negative control (PAL), studies by Peter Feaver, Peter Stein, Donald Cotter and Dan Caldwell are helpful.[51] As a whole, the mentioned experts favorably estimate the capability of U.S. C³ for reliable nuclear deterrence. They emphasize its flexibility in a great variety of potential scenarios, its high technical level – primarily in computer technology and satellite communication systems – and sufficient civilian control of its operation and modernization.

Along with positive assessments of American C³, certain doubts of its effectiveness and reliability are voiced. A number of experts criticize it for higher-than-necessary decentralization. Others express serious concerns about its vulnerability. In 1982, James P. Wade, the principle deputy under secretary of defense for research and engineering and the individual most responsible for planning U.S. strategic command modernization during the early 1980s said, "A very key uncertainty in the deterrent equation is the ability of our C³ (command, control, and communication) system to survive a Soviet first strike, and thereafter be able to get the necessary messages out to our forces to respond, to retaliate. That is an imponderable, but it is something we are very worried about."[52] Generally speaking, the gap between the opinions of American experts regarding national C³ is considerable – from very high to clearly pessimistic ones. Indirectly, this gap points to the fact that, as of this point in time, the United States (as well as Russia) does not possess a clearly-defined, widely-recognized tool for assessing the effectiveness of nuclear command and control.

In the United States, a lot of attention is paid to discussion of various concepts of nuclear weapons employment, which, in reality, means principles of command and control. Common criticism by many experts of the Russian and U.S. LOW strategy, the so-called "hair trigger," should be noted: "Serious study of various options for lowering the readiness of nuclear forces and creating an international taboo against hair-trigger nuclear postures should be undertaken."[53] The majority of experts are in favor of the LUA, or "delayed retaliation," concept as the officially recognized one. Steinbruner, Blair, Betts and Garwin made the most important contributions in analyzing this problem.[54]

Lastly, concerning purely theoretical work in this area, American and other Western scholars suggested a number of approaches to objective assessment of strategic stability, mutual deterrence and analysis of the impact of C³. Of note are the works of Elisabeth M. Pate-Cornell and P. S. Fishbeck, Steinbruner, Carter, Lebow, Bracken, Betts, Blair, as well as the material published in the collections edited by Quade.[55] The approaches

they suggest are based on game theory, on the Bayesian updating of the probability of nuclear attack, and even on common sense:

> "Yet another alternative was to assume the emerging situation to be wholly novel, forget the past, return to first principles and attempt to build up a new theory appropriate to the new age. ... The exemplary formal strategist was Thomas Schelling, with Morton Kaplan, Glenn Snyder, Daniel Ellsberg, Malcolm Hoag and Oskar Morgenstern also having a right to inclusion. The exemplar methodology for the formal strategies was provided by game theory ... One alternative was to rely on common sense – the sum of personal understanding of human nature and more immediate political circumstances – to develop judgments on how reasonably sensible and responsible national leaders might act under various scenarios."[56]

All those approaches are subjects for discussion as research tools for finding simple, reliable and truthful methods. However, the attitude of U.S. and other Western experts to the attempts of a purely theoretical resolution of the "nuclear puzzle" has until now remained skeptical.

Thus, Lawrence Freedman points out major difficulties in theory development in this field. He notes that the different indexes for assessment of nuclear balance which were used (delivery vehicles and warheads, 'equivalent megatonage' and lethality, etc.) and also the theory's problems (it is necessary to take into account a lot of factors – target structure, defects, reliability, tactics, accuracy, yield, as well as 'the lack of evidence,' or market research) used to justify the stress on *perception*. He adds:

> "Little could be known about the likely responses of human beings to any of the situations that they were liable to find themselves in during nuclear war – either in deciding whether to launch a nuclear attack, or in implementing this decision, or in anticipating and suffering the results. ... There were unavoidable uncertainties over whether it was reasonable to expect a nuclear war to have its own conventions and ground rules of the sort evident in the warfare of the past. One possibility mooted was the mutual avoidance of cities. On the other hand a nuclear exchange might be unremitting and indiscriminate. With each side able to choose from a variety of strategies there were many possible scenarios and this added further complications to military planning."[57]

Freedman also quotes Sir Solly Zuckerman from Omar Bradley's *This Way Lies Peace* (1949): "It is based upon assumptions about human behavior which seem totally unreal. It neither constitutes scientific analysis not scientific theorizing, but is a nonscience of untestable speculations about Western and Soviet block behavior."[58]

It is probably not an accident that in 1983, U.S. Defense Secretary Caspar Weinberger observed that "although survivable and enduring command, control and communications systems are decisive for deterrence and would be a critical force capability should deterrence fail, criteria used in analysis have nonetheless been blind to command and control systems."[59]

It seems that as a whole the research activity on nuclear deterrence, strategic stability, etc., including problems of nuclear command and control, has somewhat decreased in the last several years both in Russia and the United States. The Russian expert K.E. Sorokin notes: "The set of arguments on both sides has practically not changed in all this time; the conceptual level of the discussions remained the same, and the objectivity of some experts defending absolute advantages of ICBMs and SSBNs causes more and more doubts."[60]

And then:

> "At first glance such stagnation is observed not only in our country. Thus, American research publications practically do not contain any of the nuclear sophisticated research that showed up regularly in the 1970-80s. But there is a crucial difference. If here we argue about important but not the major issues, abroad they have been trying to carefully search for a nuclear algorithm of a new multipolar, post-confrontational period, to analyze – for now only in the first approximation – those characteristics that may radically change both separate components of a traditional nuclear balance and the nuclear equation as a whole. Is it not possible that early in the next millennium we will be confronted not only with a dated and worn out nuclear arsenal but also with a major delay in our understanding of the basics of the changed military nuclear situation?"[61]

Even if the conclusion about a certain decrease in nuclear research is correct, it does not mean that the importance of the problems is any less or that the dangers associated with nuclear command and control have disappeared. Therefore, initiating a search in this direction is crucial.

Unfortunately, in some cases the results of certain analyses take us too far. An article by two Russian officers, published in *Military Thought* in 1995, serves as a good example.[62] We can only welcome the audacity of their approach and broad knowledge but can hardly accept their proposed scheme of the "world order."

At first, the authors note, quite correctly, the challenges in quantitative assessment of stability and nuclear deterrence. Yet they make a methodological error: "sufficiency is a quality provided by a certain quantity. What is this quantity equal to?" And on the same page: "It is not quite clear how to calculate the needed number of strategic nuclear weapons based on the principle of defense sufficiency. How many attack weapons must one have for a successful defense?"[63]

The error is that they are looking for a quantity of weapons, not for the probability of succesful retaliation. Without this, it is, indeed, "unclear how to calculate ..." Further: "[The SNF's] only sensible role is in deterrence. The possession by a state of a certain number of strategic nuclear weapons should make the aggression against it inadmissible as such."[64]

The "only role" concept is true. But what does "certain" stand for? How and by whom are those numbers established? It is not important for the authors, since in their concept the aggression against a nuclear state is "inadmissible as such." In reality, this is a rejection of objective bases for reasonable minimums of nuclear weapons and a verdict against the methodologies for assessment of unacceptable damage. "With all seeming attractiveness of assessing stability based on the inevitability of the aggressor receiving unacceptable damage in a retaliatory strike, the impossibility to formalize this unacceptable damage makes the use of this method difficult."[65]

After such a conclusion, the authors go down the slippery slope idea of a world order supported by a group of elite nuclear states – to be more precise, Russia and the United States – also known as elitist utilitarianism. They say, "Aurelio Peccei, the founder of the Club of Rome, noticed that 'the well-being of all the world is a necessary condition for the well-being of its separate parts while the reverse is not at all obvious and should be checked in each specific case.' This statement seems reasonable and fair and proves the superiority of the utilitarian approach."[66]

True, the authors recognize "inefficiency" of a dictatorship, quoting from Pierre Corneille: "He who can do everything he wishes for – wishes for more than he should wish." Therefore, they name a system "with one subject or a group of subjects with similar goals," a dictatorial system. The authors do not explain what "goals" mean but assume that "power potential should correspond to the level of societal maturity. So, the imbalance between technical and social development may be quickly removed by speeding up societal development."[67]

We may leave the moral and political aspect of such a scheme for the "world order" and the idea of quick "leveling" of social development inside the "elite" to the conscience of the authors. In the context of this chapter, we are only interested in the absence of any approach to quantitative assessment of nuclear deterrence. Instead, the article recommends a well-known "qualitative" prescription: "... preserving equality of Russian and American potential at the levels providing for the possibility of a unilateral decision on the fate of civilization; inclusion of other nuclear states in the negotiation process on strategic weapons of other nuclear states; developing the measures for preventing proliferation of nuclear weapons."[68]

This is, certainly, a personal opinion of two officers. Yet it was published in an official military journal and is probably shared by some Russian experts. As is well-known, a number of major political and military leaders of various countries also think, often without any basis, that powerful nuclear arsenals will have to be preserved for a long time yet. Nonetheless, the search for reasonable minimums would be continued.

All of the above was only a list of authors and a summary of their main works. Hopefully, it will facilitate, especially for the Russian readers, the search for sources required for in-depth work in this field. We will later come back to the works of mentioned and other experts. In this chapter, however, it would be useful to review in greater detail those sources that, in the author's opinion, are most valid for understanding his own conclusions and suggestions.

2.2 Bruce G. Blair

One of the major studies of the influence of C^3 on strategic stability is Blair's *The Logic of Accidental Nuclear War.*[69]

The author's conclusions and recommendations are based on a significant amount of material collected and analyzed by a large group of American experts over several years. Considerable attention is paid to the historical analysis of nuclear security, including the alarming days of the Cuban missile crisis and the attempted coup in the Soviet Union in August 1991. The American nuclear command and control system is compared to its Soviet counterpart, and the book provides a large amount of information about these systems including dynamics of their development, principles of planning, composition and structure, exercises with nuclear weapons, and other data. A suggestion is made regarding a possible model for assessing the impact of early warning upon strategic stability. Many practical suggestions regarding the resolution of existing problems are reviewed.

The main thrust of the book studies accidental nuclear war. As in all analyses performed through the prism of command and control system, problems of positive and negative control are closely interrelated in this discussion. The author emphasizes the necessity of strengthening negative control:

> "The proposals require a sharp reorientation of the axes of security policies, with the emphasis tilting further away from the traditional preoccupation with calculated aggression and closer to the strengthening of safeguards against major sources of inadvertent conflict. Such rotation acknowledges that the deterrence of premeditated attack has been firmly established and that the primary threat of war arises from lapses of strict operational control over nuclear weapons."[70]

A vast range of organizational and technical suggestions for improving negative control is found in the book. One can practically agree with all of them. At a minimum, they deserve a profound study. Here we enumerate only a few of them since they will be reviewed in greater detail in following chapters.

In Blair's opinion, the top requirement is installation of reliable and easily-operated locks on all nuclear weapons: "The parties need to exchange information on the status of their respective inventories and established standards with which to evaluate the

effectiveness of existing technical safeguards. Weapons that do fail to meet their requisite standards would, by mutual agreement, be immediately inactivated (taken off alert) and slated for eventual destruction."[71]

Blair is skeptical about the idea of delegating nuclear responsibilities from political leadership to executive military units: "Numerous military nodes possess all the authorization and enabling codes needed to implement nuclear war plans ..."[72] He also notes: "One cannot fail to notice a fundamental, vestigial, inconsistency between the autonomy of the U.S. system and the international political context in which it operates. ... Such concern may be less for the Russian system because of its high degree of centralization."[73] The author, however, jokes about the Soviet command and control system: "... although the president and the defense minister have the right to order nuclear launches, top Russian military leaders have the technical ability to carry them out."[74] On both sides, according to Blair, this mechanism dates back to the Cold War and "should be subjected to presidential scrutiny and modified as appropriate."[75]

The author believes in cooperation to improve EWS, in particular creation of Russian-American center for early warning. Another idea is to install a certain combination of acoustical, infrared and visual sensors directly at the positions of ICBMs that can simultaneously send signals to warning centers, to ensure mutual confidence that the missiles remain in their silos.

Blair is in favor of more openness in C^3 than exists now: "The political revolution in the former Soviet Union has created serious problems of nuclear weapons control, but it has also brought previously taboo subjects into the public domain for serious examination."[76]

If the goal of increasing effectiveness of negative control as a whole is discussed with great clarity in the book, and the measures suggested are quite specific, the problem of positive control is presented as a complicated and ambivalent one. Concepts of employment of nuclear weapons, possible scenarios of military actions, the concept damage and related requirements to the composition and characteristics of the nuclear forces and their command and control – all of these, according to the book, are endowed not only with organizational and technical but also philosophical significance.

The author notes that, as of today, both sides adhere in general to LOW. Despite all the flaws of this concept, it seems to be inevitable, and thus to be the lesser of all evils: "Launch on warning owed its de facto adoption to the acute disadvantages of the alternatives. It represented a compromise between the extremes of preemption and retaliation after ride-out that skirted their political and technical drawbacks."[77]

Indeed, a pre-emptive strike (despite some current efforts to revive it) is a political anachronism; nor does it make any sense from the military point of view: "... the Soviets surely recognized that successful preemption would have had a negligible payoff should the United States have launched on tactical warning in response to positive indications of a Soviet missile salvo."[78] On the other hand, Blair considers retaliation after ride-out, or LUA, to be also unrealistic:

> "Retaliation after ride-out was an abstract idea in the theory of stability but not a viable option in the real world. As a practical matter, the susceptibility of command systems to disruption, the mutual vulnerability of each side's silo-based forces, and the commitment to strategic weapons targeting created a strong bias on both sides for extremely rapid reaction to evidence of impending attack – in effect a launch-on-warning posture for both sides."[79]

The absence of definite conclusions regarding the employment of nuclear weapons constitutes an asset, and not a flaw of Blair's book. The author demonstrated the true essence of this problem. He cannot bring himself to wholeheartedly embrace either of the concepts – LOW or LUA. It seems that the main reason for this uncertainty is that the bipolar (or if you want tri-polar, if we include the pre-emptive strike) theory is a dead end. Blair's book is a vivid illustration of this fact. He presents a very convincing argument that the three types of strikes follow one another in quick succession: "... the difference in release timing among all three was measured in minutes."[80] Separating these three types of strikes and controlling these choices is a challenging task. The command and control system functioning according to LOW may unnoticeably slip into pre-emptive strike without provocation, or from LOW to LUA, etc.

The author is very aware of the dangers of "hair triggers" and suggests a series of measures to help mutual reduction of day-to-day nuclear combat readiness, including command and control systems. He continues along the same lines in his subsequent works, including *Global Zero Alert for Nuclear Forces*.

I generally agree with this trend, since it will allow for the creation of a time barrier on the way to nuclear accidents. Should relations between Russia and the United States worsen again after de-alerting measures are introduced, the considerable time interval will allow "hot heads" to cool off. Still, these measures are only able to slow down, not completely exclude the return to a "hair trigger." And if this happens, the problem of employing nuclear weapons would return. Thus, the path suggested by Blair should probably be supplemented by reliable and comprehensible proof, a theoretical confirmation, that in case of deterioration of the relationships, getting back "to the barrier" makes no sense.

Blair discusses a theoretical vacuum in this area that exists at present time: "What makes a catastrophic failure of nuclear command and control particularly disturbing is that no credible estimate of the risk exists. Little more than the rough outlines of the danger is understood. A whole new kit bag of theories, tools of analysis, and data bases is needed."[81]

The idea of nuclear deterrence is a general foundation of all the approaches to the assessment of strategic stability. Blair, however, while defending the idea of "zero alert," notes that "[t]he standard deterrence perspective is more a hindrance than a help because positive rather than negative control is its main concern."[82] One hopes that Blair does not mean avoiding the assessment of positive control, but rather is wary that it

would shadow the more important problem of negative control. I feel that this is confirmed by Blair's words in the beginning of the book: "Nuclear deterrence remains a precept of both sides' security."[83]

As of now, a considerable level of trust has been achieved in relation to nuclear weapons themselves. However, the situation with command and control systems is, according to Blair, very different: "The Soviet system was particularly shrouded in secrecy. Although the successor system is now more accessible to examination, it still remains opaque to outside view."[84] The goal of overcoming this barrier is a logical step on the way to well-justified nuclear sufficiency. Blair's work will play a major role in the resolution of this problem. One may even describe it as a breakthrough.

Indeed, the volume of information on the Russian (Soviet) command and control system contained in Blair's book and the degree of its openness are without precedent. There are many facts regarding the main subsystems of command and control of the political leadership, General Staff, SNF's commanders in chief, Air Force and Navy: real names of systems, main functions and principles of employment, advantages and disadvantages. The location of central command posts, including deep underground bunkers of the supreme high command, is researched thoroughly. Unique procedures for obtaining sanctions, decision-making, developing and transmitting launch orders are revealed. Safety systems against unsanctioned use of weapons at all levels of command and control are also analyzed. For obvious reasons, the mentioned data are not complete and sometimes contradictory so that the book cannot be used as an "official reference book" on Russian command and control. Nevertheless, as of this moment, this work is almost the only open source on many issues of Russian nuclear command and control that so far have remained officially classified.

I believe that this degree of openness is necessary and sometimes even unavoidable for any serious study on nuclear security. Together with his colleagues, the author used interviews with hundreds of experts ranging from marshals, members of the Russian Academy of Sciences, and general designers, to rank-and-file people, active duty and retired military officers of missile forces, submarine units and strategic bombers. It is impossible, and makes no sense, to try and keep "the genie in the bottle," for then no research will be possible.

Having studied this book in depth, the reader overcomes the shock of surprise and becomes thoroughly convinced that opening this richness of "super secret" data does not diminish security guarantees for both parties. In spite of the fact that the data is now openly published (and for the United States this had been done a long time ago), there is no damage done. Many variable parameters of the command and control systems cannot be revealed in principle; these are current location of mobile elements, working radio frequencies, times of communication sessions, etc., since they are simulated by the opponent only with the help of probabilities, which in itself guarantees adherence to mutual deterrence.

Blair refers to this fact often: "... [t]he United States did not project a prompt lethal

threat to the deepest Soviet bunkers;"[85] "[i]t was unlikely, however, that all communications from a surviving bunker would have been permanently suppressed;"[86] "[t]he additional redundancy established during a crisis would certainly have lowered U.S. confidence in the effectiveness of strikes against the Soviet leadership and military command system;"[87] "[b]oth sides have also kept each other guessing about such critical details as plans for delegating authority to employ nuclear weapons,"[88] etc.

As a whole, it appears that the greater the openness of command and control systems, the higher the confidence in its effectiveness from the standpoint of both positive and negative control. Thus, only after encountering many examples of how the problems of negative control have been resolved in Soviet command and control systems, the author states with conviction:

> "In my estimation, the regime of existing safeguards, combined with the command system's adaptive capacity, should inspire confidence in the system's ability to endure acute domestic turmoil probably on a scale far exceeding anything witnessed to date and to contain the effects of aberrant behavior within the nuclear chain of command and throughout the life of the nuclear weapons."[89]

Blair's book is a bold attempt to break through the granite wall of misunderstanding and fear. This is its greatest contribution to the establishment of international cooperation among C^3 experts. Sadly, such an effort was undertaken, in relation to the Soviet/Russian system, by American experts and not by their Russian colleagues. This is a source of certain gaps and small errors. These have no significant impact and by no means detract from the book's general value.

Blair's work is clear evidence to the necessity of increasing contacts between American and Russian C^3 experts, both on official levels and within the framework of independent research. I think that without such cooperation it will be hard to achieve more progress in strengthening nuclear security and strategic stability.

2.3 Daniel F. Ford

Ford's book, *The Button: The Pentagon's Strategic Command and Control System,*[90] is an example of the openness with which one is allowed to talk about a national command and control system.

This work was of great interest to Soviet military leaders. In 1988, the deputy chief of the General Staff, Gen. Makhmout Gareyev, asked the Center for Operational and Strategic Studies of the General Staff to review this book. We studied the Russian translation of the book – made for a very small number of officials – that arrived in the center, made a lot of notes in the text, wrote a brief review and gave it back to Gareyev. He called the book "very interesting, worth studying carefully," but I never saw this copy of the book again.

Indeed, Ford's work made a strong impression on all of the Russian experts. We were impressed not only with the unprecedented volume of information in the field that had been "closed" earlier, but also by the degree of openness of information. We also found the style of the book – informal, dealing with real-life issues and characterized by gentle humor, very appealing. We were able to draw this conclusion from it: Americans are unafraid to talk about their command and control system because they are totally sure of its strength. That is, they are confident that the Soviets would never take a risk of checking its reliability, despite a great number of system "bottlenecks" that were severely criticized by the author.

> "According to Desmond Ball's analysis and the Pentagon's own estimates, it would take fewer than fifty Soviet weapons to disable the entire U.S. command and control system. In addition to the White House and the Pentagon, the targets of such an attack would include: the Alternate National Military Command Center, an underground facility at Fort Ritchie, Maryland, which is about seventy-five miles from Washington; Strategic Air Command Headquarters near Omaha, Nebraska; the alternate [Strategic Air Command] Headquarters at Barksdale Air Force Base in Louisiana and March Air Forces in California; the headquarters for the Atlantic Fleet in Norfolk, Virginia and for the Pacific Fleet, in Hawaii; the key AT&T switching centers – such as the ones in Lyons, Nebraska; Fairview, Kansas; Hillsboro, Missouri; and Lamar, Colorado – that handle certain critical military communications; the ground stations for key U.S. defense satellites; the very low frequency (VLF) radio transmitters in Cutler, Maine, and Jim Creek, Washington, and on the Northwest Cape in Australia (which broadcast orders to U.S. submarines): and a handful of other targets, some of which are in classified locations. To increase the element of surprise and confusion, the thirteen early warning sites used to detect incoming Soviet missiles would also be obvious targets."[91]

One would expect that after such criticism it would be possible to doubt the reliability of the American C³. But, despite these and other criticisms, such doubts are outweighed by more than 200 pages of detailed analysis, including the North American Aerospace Defense Command (NORAD); the president's dealing with nuclear weapons; rules of succession; command posts at all levels; such satellite systems as the Military Strategic, Tactical and Relay Satellite Communications System (MILSTAR), Defense Satellite Communications System (DSCS), Air Force Satellite Communications (AFSATKOM); nuclear submarine command and control through the Take Charge and Move Out (TACAMO) and ultra low frequency (ULF) transmission stations, the American Permissive Action Links (PALs), the Ground Wave Emergency Network reserve system, the Strategic Air Command's airborne command post (Looking Glass), the Emergency Rocket Command System (ERCS) system of command missiles, the

global military communications network and many other things. The mechanism of the system's operation is described for hypothetical scenarios. With such a broad and technically detailed analytical picture, the system's various faults, although quite serious, do not seem to have a decisive impact. The general impression is that the existing system has a stable "reliability zone" that needs to be periodically improved but cannot be overcome.

Despite all the problems with the Russian C^3 system, the same is true for it as well. The merit here belongs not just to both systems but also to the objects that they control – the national nuclear arsenals. Besides, "people have not yet learned how to deal with the possible fragility and ambiguities of these systems when they are under stress or attack."[92]

Ford provides a very good comparison in his book: "Without a command and control system to do all this, a nuclear arsenal would be no more useful than a fortune locked away in a safety deposit box to which one had lost the keys."[93]

2.4 Theoretical approaches

It is useful to compare opinions of certain American authors presented in the collection edited by Quade[94] and in Bracken's book[95] regarding the theoretical explanation of the role and place of a command and control system in strengthening strategic stability, with the opinions of Soviet experts in the 1970s to 1990s.

The correlation between concepts, such as sufficiency of nuclear forces and probability of their employment, is an important idea in Quade's collection. In the United States, at the time, the prevailing theory was massive retaliation, whose apologists insisted that the more horrible the threat, the more effective the deterrence. The critics of this theory argued that effectiveness of deterrence depended on the probability of the threat being carried out. An interesting thought was introduced: Sometimes, the scale of the threat may decisively reduce the probability of it being carried out.

Albert Wohlstetter, an American expert, is quoted in the mentioned book discussing the prospect that it will be impossible, due to limited resources, to provide for a high probability of preserving all nuclear forces in case of an enemy's surprise attack. The author's arguments ring true at first sight, yet they are self-contradictory and therefore interesting for the problem we are discussing. They deserve a more detailed comment:

> "Let us say, then, that we would like to preserve our striking forces with very high confidence (at least 90 chances out of 100). He [the enemy] would like to have a high confidence (at least 90 out of 100) of destroying all of our [Strategic Air Command] not certain to be handled by his defenses. Now, suppose, we have such a high-confidence measure for a certain fraction of [Strategic Air Command], and then think up another measure which gives us a 50-50 chance of preserving a considerable additional fraction. It is clear that this additional measure does not fulfill

> our fondest desires. On the other hand, it should be observed that it does prevent the enemy from having a better than 50-50 chance of realizing his fondest desires. It makes a surprise attack a gamble and *therefore acts as a deterrent.*"[96]

So far, it is logical: we would like to have more, but there is no such possibility; however, even a "fifty-fifty" deters the opponent. A notable observation follows: "One of the ways we might decrease his [enemy's] confidence with respect to the success of some particular attack strategy might be to increase the *variability* [emphasis added] of his result, even if we do not affect the average outcome. This would increase the risk for him, and might help the deterrent function ..."[97]

This is totally true: the broader the dispersion of the possible results for the risk taker, the lower his confidence. The author, however, tries to insure himself, and the next part of his argument brings up a number of questions: "... but it also means that since we have increased the variability, we have also reduced our own confidence ... Therefore our fondest desires are not satisfied. That is one reason why we continue to seek high-confidence measures for crucial goals where we do not already have them. They cannot be replaced by low-confidence measures."[98]

The following questions arise: How did he come to this conclusion? What is more crucial here – our confidence or the opponent's lack of confidence? What deters and whom does it deter? And what pair of values – "our success versus his success" – is sufficient for reliable deterrence? 90:10, 70:30 or 40:60? The author does not provide an answer to all these questions. Yet, not wishing to leave them totally open, he finishes by saying that "it is important to study systematically this less ambitious class of measures, especially where we are not able to find means of satisfying our more ambitious goals ..."[99]

We cannot help but agree. In the early stages of the nuclear confrontation (this lecture had been presented in the 1950s) both sides adhered to the principle of "the more, the better." Today, we are talking about the search for *reasonably sufficient levels of deterrence*. Or, to paraphrase it, about forgetting the "more ambitious goals" and reevaluating the significance of "low-confidence measures."

The book also, justifiably, argues that

> "This means that we have to do systems research for the enemy as well as for ourselves. To anticipate his strategy and choice of weapons we have to look at the problem from his point of view. And while there are naturally differences in the detail with which we study his problem and our own, the logic of systems research requires us to play both sides of the game."[100]

These statements should have led, inevitably, to the conclusion about the necessity

of joint research by the "dueling" sides, taking the interests of both parties into consideration. Back then, however, this joint research was impossible because of the confrontational character of political relations.

In his book, Bracken studies how realistic a protracted nuclear war is from the point of view of the attacked side's C^3 capabilities.[101] He justly assumes that evaluating the situation and making flexible new plans would be very difficult in this case because of the drastic changes in the leadership's structure after the exchange of strikes:

> "I argue that wartime conditions will impose a radically different information regime on the victim's command system. Because of the destructiveness of nuclear weapons and vulnerability of communication linkages, a command will be shattered into separated islands of disconnected forces once it is subjected to heavy nuclear attack. Each separated island then will face its own individual assessment problem."[102]

The author uses a clear matrix method to demonstrate the isolation of the "islands" of nuclear forces from their command systems. He concludes that it makes no sense to make plans for a protracted nuclear war without having a preliminary answer to the command and control problem: "Only through analysis of the assessment information available in this disconnected environment can a realistic sense of the controllability of nuclear exchanges be had."[103]

The interest in theoretical research on protracted nuclear war appears to be lower in the Soviet Union/Russia than in the United States. The majority of Soviet research on this subject concentrates on potential survival of at least one command post authorized to issue an order for the global retaliatory strike and preservation of the minimal technical means of command and control that can deliver this order to the remaining forces. This is considered sufficient for reliable nuclear deterrence. As noted earlier, the ideas of a protracted "controlled" nuclear war have been criticized in Russia.

Some other approaches of American experts to assessment of command and control systems should be mentioned here. Thus, in one of the sources dating back to the 1980s, the problem of LOW was reviewed. The decisive role of C^3 was clearly emphasized here, and, notably, the question of quantitative assessment of the deterrence factor was mentioned. Theoretically, such a system could produce enough uncertainty in a potential aggressor to deter him from attacking. Since *any* probability may potentially have this effect, the potential victim may allow, for example, for a 20 percent chance of an unsuccessful retaliatory strike and still preserve a strong deterring influence on the aggressor.

We should, however, note that when talking about a possible LOW, the author cited above never attempts to evaluate the deterrence factor in a more broad way, that is with the consideration of both LOW and LUA. Nevertheless, his next conclusion

on the role of C^3 is welcome: The vulnerability of the strategic command and control system presents a much more important problem than the vulnerability of individual types of weapons. He then states that these questions deserve much more attention than they have ever received.

In the Soviet Union/Russia, considerable attention has always been paid to assessing the effectiveness of weapon systems and scientific basis for their performance characteristics. At the same time, rational inter-relation between command and control systems and nuclear arsenals has received little direct attention, although a number of problems leading to a resolution of this larger problem have been studied rather well. This problem has received more attention in Russia in recent years.

Unfortunately, there are very few open sources on the work of Soviet experts in this area. Even though purely theoretical approaches were not (and could not) be considered classified information, they were, as a rule, presented in classified materials of military research institutions. Hence the lack of references to open sources.

Regarding the methods of selecting the indicators for the effectiveness of military automated command systems, as early as the 1970s it was noted that despite the complexity of considering all aspects of the system, a method of selecting one dominant generalized effectiveness indicator and turning all other indicators into limiters proved to be the most useful. Usually, mathematical expectation, or an average value of the damage to the enemy in a retaliatory strike, is used as a generalized effectiveness indicator for nuclear C^3 systems. Various characteristics of the damage – for example, the percent of destruction of the military economical potential -- have been used for this analysis.

Even though such indicators seem specific, it appears that they do not provide full characteristics of the predicted result. Indeed, most recommendations of the Soviet research military institutions in this area sounded like this: "In a retaliatory strike, the nuclear forces should have the capability to damage the enemy's military economical potential at the level of so and so percent." A reasonable question arises: What does "should have a capability" mean? With what probability? It is obvious that we cannot assume that this probability equals 1.0. Nothing absolute is possible. Also, such a requirement does not provide a predicted dispersion of the results. What you have here is no more, no less than a "point."

Further, requirements for command and control systems have been projected separately for LOW and LUA. It was verbalized in this way: In case of LOW, the C^3 should provide ... In case of LUA, then it should ... What does "in case of ..." mean? Nothing was ever said about the correlation between the two "arms" of the command and control system, about their contribution to the generalized indicator of the effectiveness of retaliatory actions with consideration to any potential scenario. Such a generalized indicator did not even exist.

In most research work as well as all of the official statements of Soviet (from the 1970s onward), and now Russian, political and military leaders, it has been always

emphasized that the purpose of the strategic forces is not to destroy the enemy but to deter a potential aggressor. This political principle should have been, it seems, incorporated in the actual structure of nuclear forces and their C^3 system as well as in an official substantiation of their reasonable sufficiency. Yet, the methodology even now hardly, if at all, reflects the transition from the earlier assessment of the size of the damage from a retaliatory strike to the new concept of assessment of its probability. For now, most of the talk has been about the potential levels of nuclear strikes, not about the probability of retaliation against the attacker. And if some military research works mention the requirement for the "probability of the launch orders reaching the carriers," this indicator still is regarded as a secondary one, the mathematical expectation of the damage remaining the primary one. Such requirements as "the ability of the command and control system to carry out the retaliatory actions as LOW and LUA" are still widely used, as well as the concept of "the potential survival of at least one command post," and "guaranteed preparation and transmission" of orders. All these indicators are qualitative in nature and may never be used for the quantitative basis of calculating the levels of sufficiency.

It seems that the experts from the Kometa scientific research center headed by Savin did the most advanced thinking in the methodology of assessing the role of C^3 in the mid-1980s. They used as effectiveness indicator the probability of a number of warheads, no lower than an assigned value, reaching their targets. Unfortunately, this indicator was applied only to assessing the effectiveness of just one element of the command and control system, the EWS, and not the whole system of nuclear forces and their command and control. Besides, only the conditions of LOW were considered, where the EWS parameters play an important role.

Arbatov, one of Russia's leading experts in strategic weapons and a member of the State Duma of the Russian Federation, refers to the importance of taking into account not only the size of the damage, but also the probability of retaliation, in *Security: Russia's Choice*:

> "As far as deterring a hypothetical nuclear attack, the SNF faces a double dilemma. First, what level of damage and what probability of this damage actually occurring are sufficient for deterrence? ... As far as this first dilemma goes, it is clear that the criteria of the Cold War era (destruction of up to 70 percent of industry and 30 percent of the population) are obsolete and could be reduced in the future many times over. Even under conditions of 'cold peace,' something possible in the future, a 50 percent probability of destroying 10 percent of industry and 5 percent of population appears to be more than sufficient."[104]

A logical question is: why a 50 percent probability? And which side (Russia or the United States) finds this probability sufficient? Regarding this Arbatov says: "As dem-

onstrated by years and years of research and debates, it's difficult to calculate these criteria 'objectively' and prove them rationally. The solution is that political leadership, on the basis of common sense, should come up with a qualitative definition."[105]

Of course, even in this case deterrence should be estimated on the basis of common sense, but if any concrete probability value would be mentioned, it should be calculated and justified. Especially since, as Arbatov concludes, the qualitative definition, accepted by political leaders on this basis, "... will determine many things: the number of warheads that must survive enemy attack, get through the enemy's BMD (possible in the future), and reach assigned targets, and therefore determine the general number and composition of strategic nuclear forces for the corresponding period of time."[106]

The ideas of Carter in a 1987 collection published by the Brookings Institution deserve a special consideration.[107] They coincide, to a considerable degree, with the ideas developed in the following chapter and represent a broader theoretical context for the method of assessing the C^3 contribution to nuclear deterrence.

In his work, Carter considers all widely-dispersed results of a nuclear operation, or as he refers to it, error and uncertainty – that is the aspect which most analysts are reluctant to study: "From the beginning one must face the fact that the specific instances of error and uncertainty almost always look improbable and absurd, which threatens to discredit them as subjects for serious study."[108]

The author says that it would be preferable to know not only the most probable value of the final result but also its range of possibilities as well as the relative probability of all outcomes:[109] "Dramatically different outcomes might not be downright unlikely, but only less than the expected outcome. The expected outcome, though the most likely, might nonetheless be unlikely ... Most sinister of all, but almost surely present, are the 'unknown unknowns' of which operational planners are not even aware."[110]

Let us remember that we are talking about a potential outcome of a nuclear war.

It is also noted that the range of possibilities of a large number of independent events is usually not great. Here Carter is discussing a range of possibilities, between 3 percent and 5 percent in the example of launches of combat missiles in the course of a hypothetical nuclear strike. Doing this, he considers previously obtained data from experience, including data from missile tests.

Later, however, he suggests also that there are factors that have much more influence on this range of possibilities: EMP weapons, EWS, C^3 and others. In some cases, it is possible to isolate one of these factors and study its influence on the final outcome. This type of research, however, is not to the liking of some customers from the military and political leadership:

> "Frank discussion of uncertainty can also be mistaken for stupidity or political circumspection on the part of the analyst. In the words of General Estes, 'Any analyst who told a general or a Congressional committee, that a weapon system would have

> a survival probability of between 10 percent and 100 percent would be drummed out of the analysts' corps and his viewgraphs would be burned to avoid spreading the infection'."[111]

(This sounds like the Middle Ages! Try to analyze and suggest anything after this ...)

Nevertheless, this approach appears to be the right one because we are talking about nuclear war, and the price to be paid for its "least probable" outcomes is extremely high. The method described in the next chapter is based precisely on researching all possible outcomes of nuclear retaliation. Estimation of these less probable (but still unacceptable because of the size of the damage) outcomes is the essence of taking into account the C^3 factor when providing a quantitative assessment of nuclear deterrence. Let them be unlikely – but they are still *unacceptable*. If such a probability cannot be completely ruled out, then *any* attempt to test this assessment in practice is unacceptable *in principle*. What could be simpler? But unfortunately, until now this approach has been practically ignored by official studies.

Carter feels that not everything is lost yet: "Concern about error and uncertainty can appear to those who manage nuclear operations as implied criticism or distrust of the deterrent 'system.' Assimilating error and uncertainty is probably easier for political leaders than for 'experts.' Politicians know how wide the gap can be between plans and reality."[112]

To sum up, the sources reviewed here allow one to conclude that both Russia and the United States have paid certain attention to the influence of command and control systems on strategic stability. American experts have placed a greater emphasis on these problems. Nevertheless, even today we lack a clear and well-substantiated methodology for a quantitative estimation of the C^3 contribution to nuclear planning. Such a methodology could facilitate more rational planning of future nuclear arsenals and their further reductions.

Chapter 3

The Methodology: The Estimate of Nuclear Deterrence Using C^3

This chapter describes one possible method for assessing the effectiveness of nuclear deterrence. Notably, it takes into account the effect of all aspects of a nuclear C^3 system under attack – its structure, reliability and principles of operation – upon the final result of any retaliation.

The proposed logical and mathematical approach was developed from 1987 to 1990 at the Soviet Center for Operational and Strategic Research of the General Staff. Using this approach, the author, together with experts from the General Staff, SRF, research institutes of the Ministry of Defense and defense industry design bureaus, carried out a number of official research projects dealing with nuclear deterrence, strategic stability, defense sufficiency, etc.

This methodology was described in detail in the book, *The Assessment of Guarantee*, written on my own initiative in 1991, while I still worked at the Center for Operational and Strategic Research. Three years later, it was published in Russian by the Moscow Institute of International Relations[113] with the only changes the substitution of the word "Russian" for "Soviet."

I had two reasons for changing so little. First, I wanted to preserve the style of the original manuscript, which reflected, to a certain degree, the spirit of military research during that complicated historical period and of hope for the success of *perestroika* in the Soviet society. Second, I wanted to demonstrate that the method offered in 1991 still applied not only in 1993, but for the foreseeable future as well.

Here, I have decided to use the same decade-old style to introduce an international readership to the essence of this method, as it appeared in the full text of *The Assessment of Guarantee*. As a result, Chapter 3 is more difficult to read than other chapters in this book, and there may be some repetition. In my opinion, however, these shortcomings should be compensated for by the integrity and simplicity of the material.

3.1 How Does Deterrence Work?

Obviously, strategic stability, safety, balance, parity, etc., rest on the foundation of nuclear deterrence. Over the last 40 years, deterrence has considerably helped maintain peace on Earth. The very character of nuclear weapons predetermines a primary role for deterrence; this will remain so in the future even after deep reductions in U.S. and Russian nuclear arsenals. The further the process of disarmament goes, however, the more important will the quantitative aspect of deterrence become.

Let us review briefly the nature of nuclear deterrence. This review will only include the military aspect of deterrence, ignoring political, social and human motivations. What prevents nuclear antagonists from starting a nuclear war? To simplify matters, we will only discuss two sides, even though all following statements and conclusions are, in principle, applicable to most members of the "nuclear club." Imagine a potential aggressor who would like to achieve his goal with the smallest damage to himself and by way of a sudden nuclear attack.

So, what *does* deter him?

As of today, huge arsenals of nuclear weapons have been accumulated. These arsenals are so immense that their owners consider it possible to start cutting them without having compared the projected results of a hypothetical nuclear conflict. This logic is simple, and, to begin with, is correct: if the level of potential harm to the other side is so high, it is possible to start decreasing arsenals without any major risk. The cuts are largely planned based on comparing the arsenals: you have 6,000 nuclear warheads, and so do we.

But what then? A simple parity of arsenals would not be sufficient for planning an attack and response – there is no measure of the capabilities behind the arsenals. With

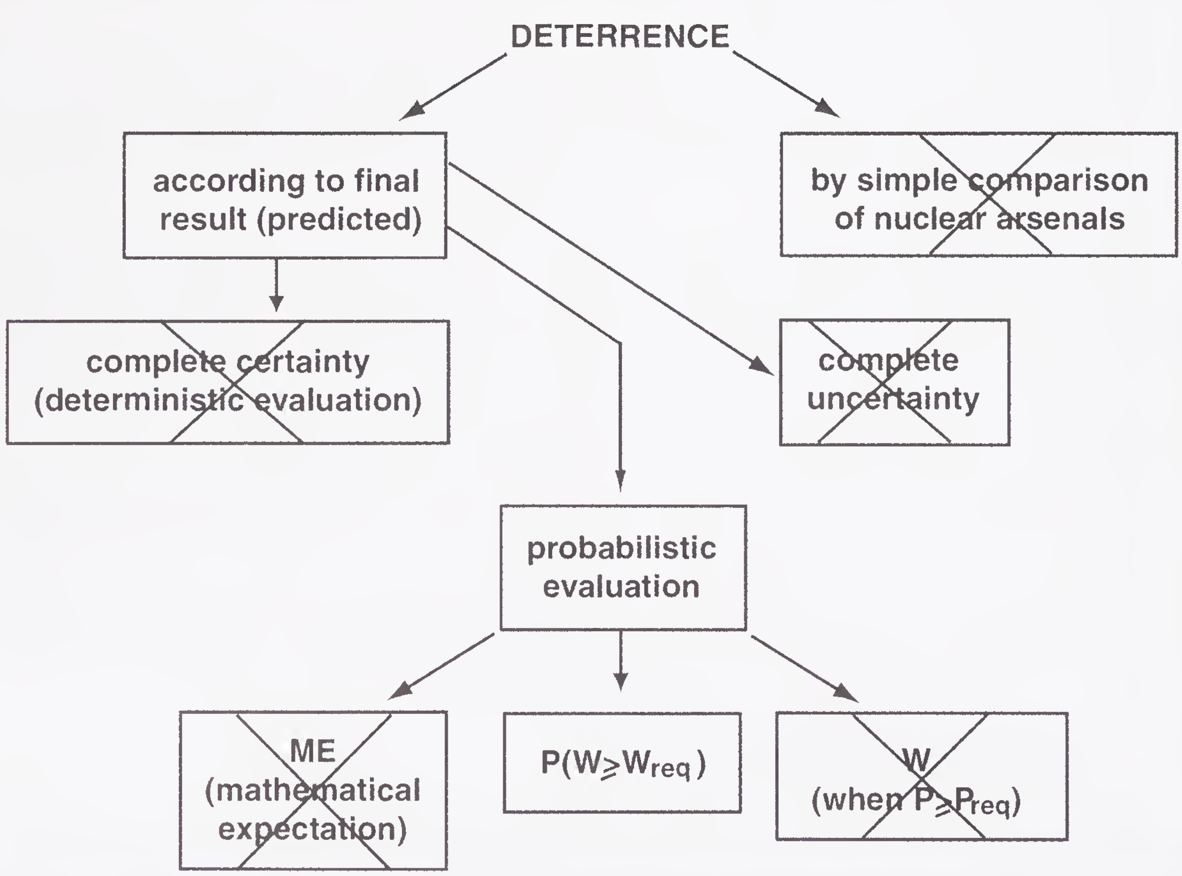


Fig. 1: Alternative methods for estimating reliability of deterrence.

this kind of "methodology," there is a chance that one side, or maybe both, may cross over a dangerous line in reducing the number of weapons – that is, beneath a minimal deterrent parameter.

Fig. 1 demonstrates possible ways of evaluating the degree of nuclear deterrence. Considering all of the above, it is necessary to stop simply comparing potentials. There is an alternative: studying the expected result of retaliatory actions on each side if it were attacked with nuclear weapons. If the risk from such retaliatory action for the potential aggressor would be such that it would provide reliable deterrence from an attack, strategic balance, parity, safety and stability would follow. The size of nuclear arsenals thus becomes a secondary factor, even though it is still desirable that they are as low as possible.

What is the nature of a nuclear conflict's projected result? And how should it be assessed by a potential aggressor considering a surprise attack?

First, the aggressor would need to use an integrated approach toward such an evaluation. He should include in his calculations not only the potential damage from the opponent's retaliatory actions, but also self-inflicted damage from his own attack (such as environmental, etc.). The trend in nuclear development, however, is now toward high precision and relatively low-power weapons, which will serve to reduce environmental damage, especially within the framework of general arms reductions. Therefore, the main emphasis should be placed on evaluating the damage from an opponent's actions.

Second, the potential aggressor should consider that, in retaliating, an opponent would use the major part of his nuclear arsenal; that is, would attempt to deliver a massive nuclear strike. The targets of such a strike would include not just military targets on the aggressor's territory but also administrative centers, industry and so on. Thus, the response would by all means have the character of retaliation. A great deal is being written now about "reasonable" or "acceptable" levels of damage in a nuclear attack. This is a complicated question, and the assessment of what is "reasonable" or "acceptable" fluctuates widely. Nevertheless, independent of the assessment method, these levels have to be fixed at a certain value. Otherwise, it would be impossible to carry out any quantitative calculations. Considering this, we will later review the concept of "unacceptable damage."

Third, when assessing the degree of risk, we by all means have to include one circumstance of key importance for clarifying the approach described in this book. Until now, we have been talking about the *magnitude* of the damage of any retaliation. But this does not include all aspects of danger or risk. The potential aggressor would very likely be interested in another, equally important, aspect of the danger of retaliation with major consequences: how *probable* is it? In other words, what is the probability of suffering unacceptable damage as a result of one's own aggression?

As of today, unfortunately, probability has been ignored as a variable in nuclear planning. The magnitude of damage is sometimes expressed by a statistical median value

or mathematical expectation. Yet, this does not change much, because it still is unclear what the probability of such a danger is. At the same time, this seemingly abstract parameter (probability) has a specific financial character – it will cost a certain amount of money. The higher the forecasted probability of retaliation that the potential victim of aggression is trying to achieve, the more expensive the retaliatory capability becomes. For example, a probability of 0.5 costs 2 billion rubles while a probability of 0.7 costs 4 billion rubles, etc. This correlation will be analyzed in detail later. Here, we will just note that "highlighting" this aspect of danger has both strategic (deterrence) and economic (cost) importance.

For further clarification of this method of evaluating deterrence, it also would be helpful to consider the random character of the result we want to predict in more detail.

3.2 How Random is the Final Result?

It is not at all simple to address randomness in the outcome of the victim's retaliatory actions. Frankly, the potential aggressor cannot predetermine with any certainty that he will not be subjected to retaliation, nor can the potential victim determine whether he will be able to retaliate.

Today, everything is based on complete uncertainty – simply on the fear of a nuclear apocalypse.

Some insist that this vagueness is a powerful deterring factor in itself. No one doubts this, especially today when nuclear arsenals are so huge. So, should we just stop here and do nothing?

We will not be able to. Technical progress is relentless. Politically, people have dared to start reducing nuclear arms, and it is hard to argue against this general trend. In military and technical areas, the means for attacking nuclear arsenals are being continuously developed and improved. Put together, these two factors – political and technological – will gradually bring us to a point beyond which deterrence may not work. We can call this a fatal point without any exaggeration. What is its nature?

If we do not try to search for this point, we will be confronted by two dangerous extremes on the difficult path of nuclear arms reductions.

One extreme is that "risk-takers" in the potential aggressor country may insist that the risk of retaliation is not high, and "expect" to resolve all problems with a surprise nuclear attack without entailing any serious damage to their own country. This trend is increasing as conventional weapons become more powerful, especially in euphoria after victories in local conflicts such as the Persian Gulf War. The thought process would be something like: "let's take a risk, nothing terrible will happen!" There is no need to explain the consequences of such thinking.

The other extreme is being overcautious. Sensible people will object: "is it really possible to talk about 'unnecessary' caution with regard to a nuclear conflict?" But let us reserve judgment. We must beware of being overcautious. The very nature of such concepts as disarmament, security and sufficiency implies striving not for minimum

levels of nuclear deterrence, but rather for "reasonably" minimal levels. And "reason" implies, first and foremost, a quantitative assessment. It is hard not to quote Lord Calvin: "If we are not able to measure a phenomenon quantitatively, we know nothing about it." That is, we have to learn to measure the deterrence factor. Otherwise, we will spend huge amounts of money in a hare brained manner, and our resources are limited.

Possibly, the above arguments are enough to convince ourselves that we can no longer live in an atmosphere of complete uncertainty. That is why this path is crossed out in Fig. 1. Let us now try to establish to what degree we may be able to use quantitative measurement in this case.

Initially, we must ask whether the desired result of retaliation is predetermined, whether it has a fixed value under certain specific conditions. Or, is it at least possible to express it by a relatively stable median value, with a small range of spread? In order to answer this question, it is necessary to turn directly to the object of research, that is, the nuclear capability of the "potential victim" and the factors that affect this capability in case of retaliatory actions. Consideration of this data should emphasize their influence on the spread of the values of the final result. If the spread is not too great, we may use the median value (so-called "determined" evaluation). If the spread is great, this method cannot be applied.

It is interesting that the United States considered the spread of the potential retaliation values as important even in the beginning of the nuclear standoff. Here, and later, we will be referring to Analysis for Military Decisions, edited by E.S. Quade, translated and published in Russia in 1969.[114] The book contains a series of lectures delivered by leading experts from RAND Corp. for high-level Defense Department and industry employees in the United States. Even though some of the ideas are clearly dated, others are still relevant.

On the issue of the spread of results, the book says that the greater the spread, the better for deterrence. The use of the words "to increase" in relation to the spread of results, however, implies that the authors desired to increase this range artificially. In reality, we will show that it is achieved "by itself," under the influence of certain objective factors.

There are many factors affecting the range of final results, and there is no need to name all of them here. It is more important to divide them according to the character of the effect they have. Here are the major ones.

Factors of the first type are those that do not have a major influence on the spread of the summary final result, but rather establish its absolute value. These include the survivability of specific nuclear weapons platforms such as missile launchers, submarines and strategic bombers under attack by conventional and nuclear weapons. The ability of missiles and warheads to overcome the opponent's BMD is also included here. Also, among these factors is the coefficient of combat readiness of each delivery system, which integrates the equipment's technical reliability with the morale of the

launch crew, etc. These factors all share one characteristic: each one is manifested individually for each SNF element (missile launchers, submarines, planes, etc.), or even for each warhead. The sum total of the state of these elements (survival or destruction) is represented as the sum total of a large number of independent variables. In other words, these variables are weakly correlated. An integrated assessment of the sum totals of such variables is successfully carried out using median values (mathematical expectation).

Most of the factors that influence the final result belong to this first group. Their combined effect should lead to some kind of a median final result. For example, we may assume that initially the attacked side had 1,000 delivery vehicles with 6,000 warheads. Let us assume that the loss of delivery vehicles in the conventional conflict was 20 percent; in the nuclear conflict – 30 percent; the coefficient of combat readiness was 0.9, and the opponent's BMD had 30 percent effectiveness. Through a simplified calculation we may presuppose that about 2,000 warheads will reach their targets in the retaliation phase. Even when considering that the mentioned factors and the calculations are much more complicated than presented here, it is still possible to express the final result by a "point value" – about 2,000 warheads – without a major error. Let us repeat that this result would be possible only if the state of various SNF elements had been considered independently from one another. In reality, this is far from being so, which makes the character of the final result quite different.

A second type of factor is different in principle in as far as the influence it has on the final outcome. As a result of this factor's impact, the spread of possible values for warheads that reached their targets becomes very large, from zero to a certain maximal value (based on specific initial data). This factor is called the *command and control system*.

The question of what influence command and control systems have on the final outcome of retaliation that we want to forecast is the main thesis of this book. At this point, we are only assuming the impossibility of describing the final result with a fixed deterministic value. Although this conclusion is obvious, we will try to clarify it in the next few paragraphs.

Thus, we cross out another method – deterministic evaluation – in Fig. 1. Only the third, intermediate version is left – the *probabilistic* evaluation approach.

In his day, when Albert Einstein became familiar with Heisenberg's indeterminacy principle, he told his friends that he could never accept it. He could not believe that God based everything He created on a probability principle; that God "played dice."

The question we are considering is somewhat similar. We are trying to assess deterrence by way of probability. You might answer: "probability belongs with indicators characterizing a process that can be repeated many times, while nuclear war can happen (God forbid!) only once." How to deal with this contradiction?

There is no contradiction here since we are dealing with simulation. You can play war as many times as you want using a model, and thus obtain any distribution of ran-

dom results depending on initial data. You may obtain the values of the probability indicator you are searching for.

Nevertheless, the question remains – how is it in reality? We would have one and only one "try." How can we evaluate the danger on the basis of only one try? Even with this one try, the result may be anything – from zero to the maximum. Our one and only try is unpredictable, and that's a fact.

So, how do we reconcile multiple simulations with only one try?

The answer is simple. The potential aggressor considering this try is evaluating the results of simulation. This situation is reminiscent of an attempt to get a ball of the required color out of a bag. Say there are seven white and three black balls in the bag, where white is life, black means death. The probability is 0.7. Another scenario: nine white balls and one black. Is there a difference? Yes, there is. But, you still do not feel like trying to get a ball even in the second scenario, especially when the risk is not just personal, but threatens our whole civilization. On the other hand, billions of rubles or dollars are behind these numbers. So, no matter what, we have to learn to accept these numbers and this approach, if only because there is nothing else.

Let us make some intermediate conclusions here:

1. Deterrence is determined not just by the magnitude of retaliation but by its probability as well.

2. The magnitude of retaliation is a random value with a considerable spread – from zero to a certain maximum. The factor "to blame" for this spread is the command and control system.

3. As of today, we do not know the nature (or law) of distribution for the random magnitude of retaliation. Deterrence is based on complete uncertainty, that is – simply on fear.

4. If we want to search for a reasonable level of nuclear sufficiency, we have to move away from this uncertainty. If we do this, we will gain a chance to compare and evaluate appropriate costs even with the most approximate quantitative indicators.

These are only initial conclusions, yet on their basis we can begin to discern the general shape of the suggested approach. The problem is: describe a hypothetical nuclear conflict using classical probability theory and mathematical statistics. Notably, most research in this area also attempts to solve this problem. There is nothing new to the question. The "only" difference in the suggested approach will be how to evaluate the influence of command and control systems on this process, and how to describe and apply any results. From this point, we will concentrate our attention on these aspects of the problem.

3.3 The Essence of Approach

3.3.1 The Object of Study

Since we are evaluating one side's ability to respond to an attack by another side, the object of our study will be the complex of systems used for such a response. We will view the defending side as the object of study, and the attacking side as a set of impacting factors using the appropriate initial data.

Let us assume that Russia is the defending side, while the United States is an attacker. Now we have to estimate the level of deterrence required to keep the United States from attacking Russia by analyzing the degree of likelihood of an unacceptable (or given) retaliation. Naturally, this approach implies an estimate of the reverse: deterring Russia from an attack against the United States, conducted in the same fashion. The indices obtained as a result may be different, but together they determine the balance of mutual deterrence.

What is included in the object of study, i.e., the complex of retaliatory systems on the defending side?

First of all are the components of the nuclear arsenal, ready for use: SRF silo-based and mobile launchers; SSBNs, which are the naval component of the SNF (NCSNF); and strategic bombers (SBs) carrying nuclear weapons.

These nuclear weapon delivery systems (DSNW) are armed, depending on their type, with various numbers of warheads (WH) each. When calculating the generalized final result, we will use the total number of warheads delivered in a strike (N_{wh}). Below we shall investigate the separate question of deriving the magnitude of damage from the number of warheads. The N_{wh} value will be used in a general demonstration of our approach for reasons of simplicity. Thus, the first element of study is the delivery systems deployed to different areas (zones).

The second element is the SNF C^3 system. Since the C^3 system will be described in some detail later, here I will provide only its general contours. C^3 includes all those subsystems that provide for the following: delivery of information about rocket attack and nuclear attack (RA and NA) from global information systems (GIS) to the NCA; NCA decision-making to use nuclear weapons, and transmission of the corresponding authorization to the highest level military command posts (HLMCP). These are the command posts that have the mandate to prepare and release execution orders, either with authorization from NCA or autonomously, under a certain set of conditions signifying nuclear attack. And finally, communication channels for transmitting orders from HLMCP to the nuclear weapons delivery systems.

The third element of study is the global information system (GIS), which provides strategic nuclear C^3 systems with data about missile and nuclear attack. The data concerning rocket attack come from the missile attack EWS, while data concerning nuclear attack come from a system that identifies numerous nuclear detonations on Russian territory.

The simplest graphic view of the object of our study will be:

Fig. 2: The object of study.

3.3.2 Factors of Influence

Generally speaking, influencing factors can be divided into two groups: internal and external. Internal factors are technical reliability, readiness of launch crews, etc. However, it is more convenient for us to take these influences into consideration when preparing initial data for the elements of our study. Thus, we shall assume that the only influencing factors are those directly related to the attacker. These factors are:

- the physical impact of various types of conventional (non-nuclear) weapons upon all elements of the object of study, i.e., upon nuclear delivery systems, command facilities, relay facilities, means of observation and intelligence;
- massive nuclear strike against these same elements;
- electronic suppression of information and command and control channels between the elements of the object of study.

This could be graphically presented as follows:

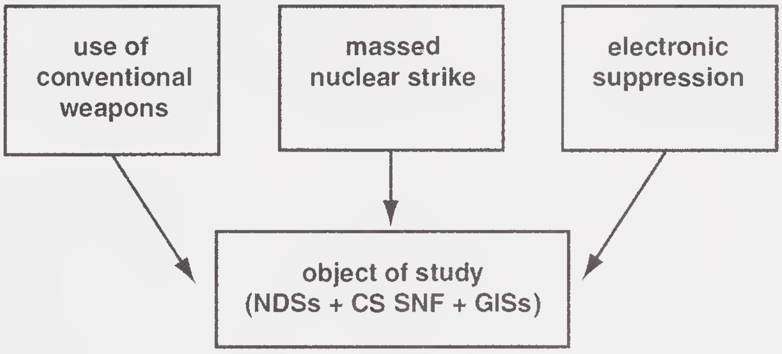


Fig. 3: Factors of influence.

In principle, one may take into consideration other factors, such as electro-magnetic pulse (EMP), beam weapons, etc. From the viewpoint of methodology, this is not important.

3.3.3 The Model

In reality, this will be a complex of models linked by a common concept and algorithm. The general idea of modeling here is to "play" war a certain number of times and attempt to determine, with an acceptable degree of accuracy, a distribution of the possible magnitudes of retaliation against the aggressor. In other words, it is an attempt to determine the value of the degree of risk.

The best means for solving this problem is a statistical imitation model (SIM), which does not require high accuracy. From the standpoint of risk estimate, it is not necessary to compare such probabilities as 0.72 and 0.74, or 0.50 and 0.53. For practical purposes, it is sufficient to compare such probabilities as, for instance, 0.4 and 0.7. Thus, the required accuracy can be achieved in SIM by a reasonable number of "tests." The accuracy of the initial data in SIM is another matter to be dealt with later.

Application of SIM has the clear advantage of a conditional analog of the process under investigation, which takes into consideration all major factors and allows us to obtain a probabilistic distribution of the random resulting value, rather than an "abstract" point estimate. We must model the following main stages of nuclear conflict:

- a nuclear missile attack (possibly following a conventional war);
- information the Russian NCA has about the missile attack (mostly on the basis of data from the early warning system);
- the NCA's decision to use nuclear weapons, and transmission of this decision to the HLMCPs;
- receipt by surviving HLMCPs of information about the nuclear attack directly from the system that observes nuclear detonations on Russian territory;
- preparation by HLMCPs of orders to unblock and use nuclear weapons (NW), and transmission of these orders to C^3 system channels;
- transmission of orders directly to nuclear delivery systems by the C^3 system while under enemy attack;
- launch of missiles, and warhead impact on the aggressor's territory.

The final result of each computer-simulated "test" will be the total number of warheads delivered on target N_{wh}. The final result of *k* tests will be the probabilistic distribution of the value N_{wh}. Thus, this model should take into consideration the dynamics of conflict.

Despite the considerable complexity of taking into account all factors, such models exist and are successfully used in research. Because of a number of simplifications and conditionalities, they have an aggregate character.

Our model has all the elements under study presented as a so-called cohesion graph, that is, a net of nodes with arcs connecting them. The node producing initial information should be called the initiator. In our case, it is a single, abstract node, imitating the attacker's missile launch. The final nodes are the information addressees – the nuclear

delivery systems. There are many of them, reflecting the character of the grouping of strategic nuclear forces. All the intermediate nodes and arcs serve to imitate the processes of preparation and transmission of intermediate (secondary) information.

An attacker's missile launch "generates" information about a missile attack, and later, about a nuclear strike; this information, in its turn, is transformed into an NCA decision, and action by HLMCP crews. Orders issued by HLMCP and the degree to which they reach nuclear delivery systems determine the resulting value N_{wh}.

The attacker conducts a suicidal experiment: he starts the mechanism that may kill him, or may not. In order to reduce the probability of his doom, the attacker attempts to have an impact upon all the nodes and arcs of the graph (naturally, except for the initiator node). This impact may be through use of conventional and nuclear weapons, as well as through electronic warfare. Our modeling should determine how much the potential attacker can reduce the degree of risk.

The mechanism for such a SIM is relatively simple. Each node and arc is assigned probable-time functioning indices, i.e., the probability that each one of them will func-

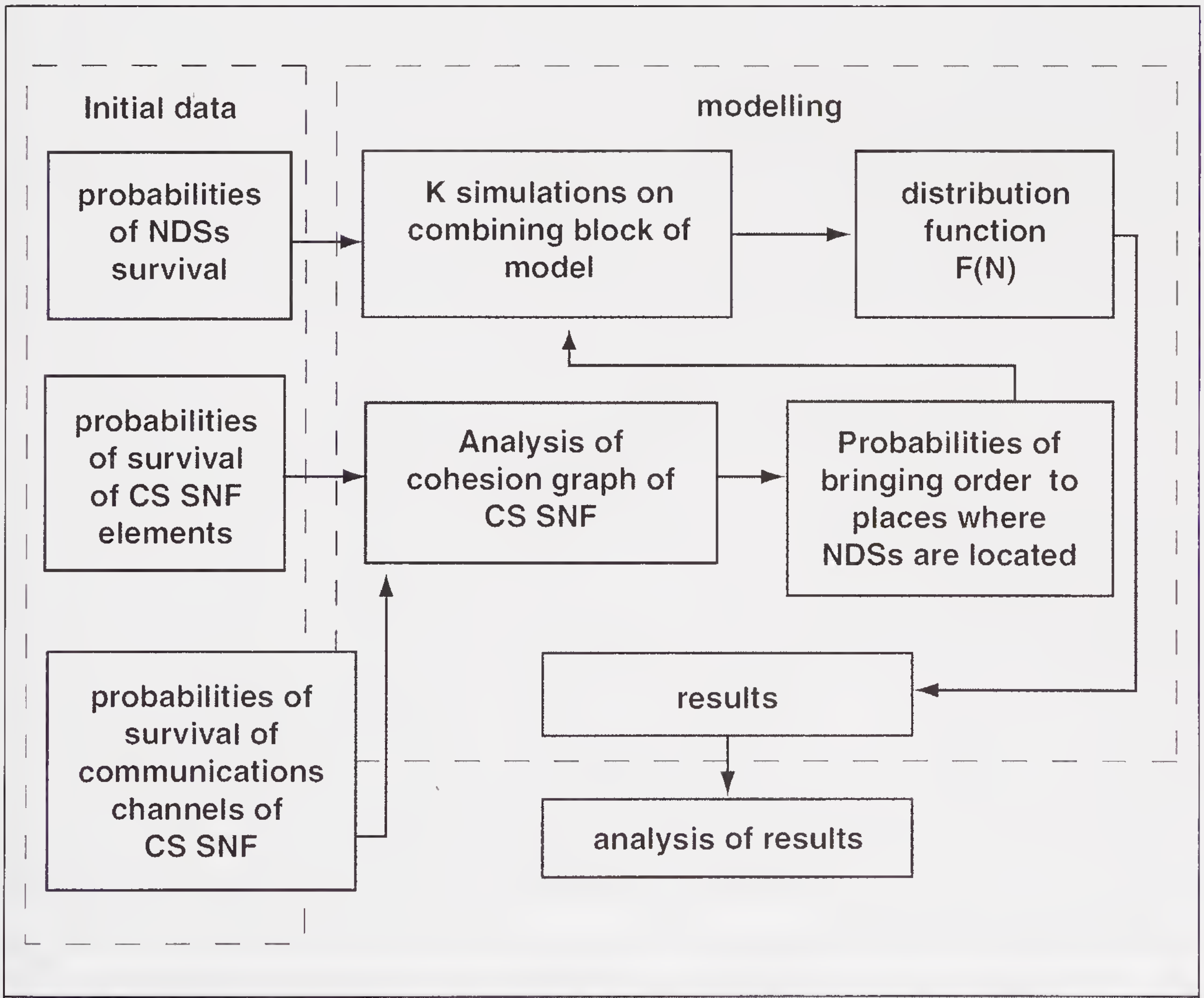


Fig. 4: Model for estimating CS SNF (command structure of strategic nuclear forces) effectiveness.

tion properly during the time period Δt_1, Δt_2, Δt_3, etc. The values of these indices depend upon the characteristics of the node (or curve) and the degree of the attacker's impact upon it. The result of such an impact is to slow information down in the net, to a different degree in different tests. There is also an impact on the addressees themselves, the nuclear delivery systems. For each delivery system, the model analyzes one situation: did the delivery system receive an order and launch before it was destroyed? For each war simulation, the number of such delivery systems is calculated, and so is the total number of their warheads; the losses from enemy BMD are taken into account, and finally the value N_{wh} is determined. In each simulation, as we have said earlier, this value is different. After *k* simulations, we obtain a probable distribution, i.e. a certain (for the given set of initial data) statistical series.

The final result is totally dependent on the values of probable-time indices of nodes and arcs. The latter, in their turn, depend upon the attacker's impact. It is only natural that the attacker would design his impact strategy in a way allowing him to allocate his realistically limited arsenal optimally – in order to get the "best" outcome. We shall discuss this outcome that later. Let us conclude that the attacker would attempt to optimize his strategy based on an expected final result. Naturally, we must foresee this, and base our calculations on the optimal (for the given set of basic data) strategy of impact.

3.3.4 Presentation of Final Results

After *k* computer simulations with one set of basic data, we obtain a mass of random values of the final result as *k* values of N_{wh}. This is the so-called statistical series.

Let us take a simple example with a small number of computer simulations, for instance, *k*=10. Assume that after 10 simulations the following values of N_{wh} are obtained:

SIMULATION NUMBER	N_{wh} VALUE
1	100
2	50
3	43
4	80
5	0
6	110
7	60
8	0
9	48
10	74

Table 1: Results of ten simulations.

How to analyze these results?

As noted earlier, there are two aspects of risk for a potential attacker: the magnitude

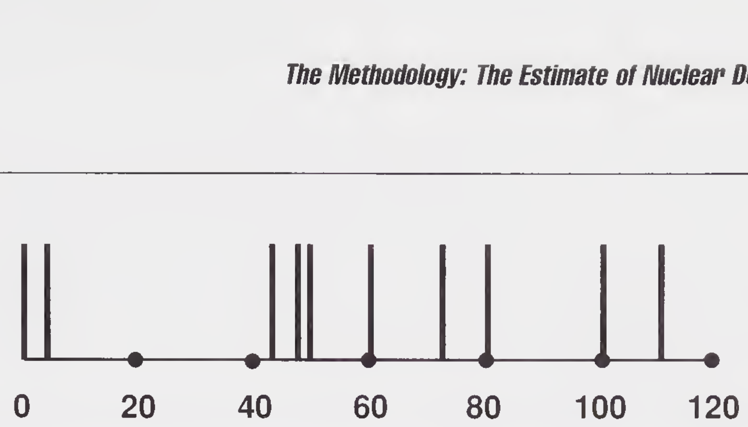


Fig. 5: Mass of results

of retaliation and its probability. Therefore the aggressor should initially determine the magnitude of unacceptable retaliation. If we assume that unacceptable damage $N_{ud} = 50$ warheads, then all $N \geq 50$ will be unacceptable.

Addressing the probability of the risk, the potential attacker will want to know how frequently $N \geq 50$ could occur. (This "frequency," naturally, is applicable only to modeling!) Our results show that out of 10 cases, six were $N \geq 50$.

As the number of simulations in SIM increases, the frequency of the given event begins to approach its probability. We will therefore speak not of frequency, but of probability. Thus, in this particular case one may say that $P(N \geq 50) = 0.6$.

If $N_{ud} = 20$, then $P(N \geq 20) = 0.8$, and $P(N \geq 100) = 0.2$, etc. Taking into account that N_{ud} is quite uncertain, it is more convenient to present the results in a table:

N_{ud}	20	40	60	80	100	120
$P(N \geq N_{ud})$	0.8	0.8	0.5	0.3	0.2	0

Table 2: Probabilities of different levels of retaliation.

A warning is due here: the probability values reflect not point final results, but probabilistic fields of results! Thus, for instance, 0.5 is the probability that the strike may have any magnitude no less than 60 warheads. In our case, these are strikes of 60, 74, 80, 100 and 110 warheads. It would be absolutely wrong to say that the probability of a strike of 60 warheads equals 0.5.

The table does not show a strike with a magnitude of 0 (zero), although in the final distribution it occurs twice. Why? Because it makes no sense to speak about $N_{ud} = 0$. Similarly, it makes no sense to search for the value $P(N \geq 0)$, since this probability obviously always equals 1. Here we are dealing with a special "borderline" point zero. Its probability is quite important for us, and we must be aware of it. In our case we obtain: $P(N=0) = 0.2$.

Now we should address the distribution function F(N). It is a graphic representation of the above-mentioned table.

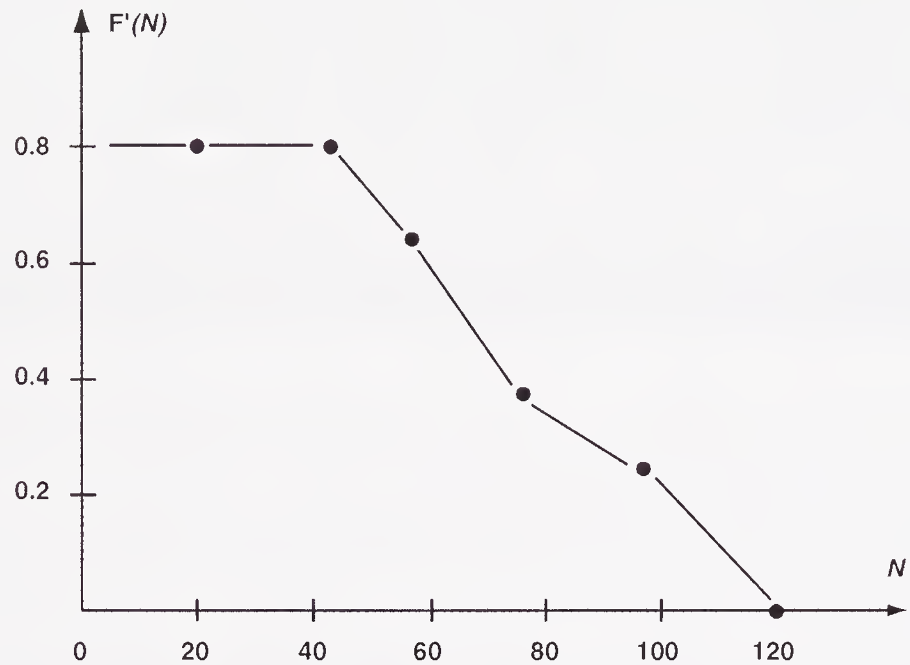


Fig. 6: Distribution of modelling results.

One may object that this curve was demonstrated by Ye. S. Ventsel' as going downward, and not upward, as in our case. But the classical distributive function concerns a "no more than" type of event, while we are interested in damage *no less than* assigned. We are dealing with reverse function F'(N), which does not change the substance of the matter, because this function has all the same properties as the classical one.

$$F'(N) = 1 - F(N)$$

Letters F and P have significantly different meaning. For instance, F'(N) denotes simply the whole distributive function. F'(N = 20) or simply F'(20) is the value of the function F'(N) in the point N = 20. This value in the given point is 0.8. But isn't 0.8 a probability? Yes, it is the probability of N being *no less* than 20. In other words, F and P are linked by the following dependence:

$$F'(N = 20) = P(N \geq 20)$$

That is, the value of the function F'(N) at the point N = 20 is nothing but the probability that N will be no less than 20.

These are the basics of probability theory, and they are given here only to avoid

misunderstandings while considering the practical aspects of the proposed approach. This is the mathematical foundation of our approach.

We will be using more graphs further on, where the Y axis shows the values not of F'(N), but of $P(N \geq N_{req})$, and "req" is "requested." In some cases, it will be more convenient to substitute for the graph of distributive function the corresponding graph of distribution density $f(N)$. Since we will have few simulations, this will be a discrete statistical series. In practice, when the number of simulations is large (>100), it is more convenient to use a continuous graph of distribution density instead of discrete series. If applied to our study with a large number of simulations, this graph might look as follows:

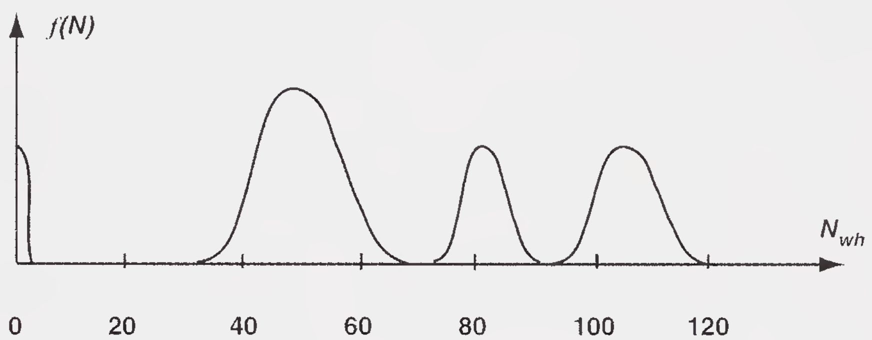


Fig. 7: The density of distribution of modeling results.

The distributive function, or density of distribution, characterizes most completely a random value. But using them in practice is not altogether convenient. It is necessary to use the corresponding simpler and more demonstrative index $P(N \geq N_{req})$. This one is most convenient because it responds to the question of deterrence: what is the probability of unacceptable damage? We will refer to this index as the degree of risk or deterrence index.

At the same time, the distributive function obtained can provide us with other indices. Two of them, together with the one mentioned above, are most well known: mathematical expectation (average from all results), and the index of value N when $P \geq P_{req}$. This last is unlikely to be convenient for frequent use, since today most studies rely upon the concept of unacceptable damage, although its value has not been determined yet. Nevertheless, the converse problem to find the value under conditions of a probability not lower than that assigned ("requested"), may be viewed as only subsidiary.

Mathematical expectation is a different matter. This index is the most usable now, although it has a number of shortcomings. Later, we will investigate these shortcomings and demonstrate why the proposed deterrence index $P(N \geq N_{req})$ is more preferable for analyzing the problem of sufficient deterrence.

3.3.5 Application

We have considered the process of estimating one concrete data variable. The result of

this estimation is expressed by the distributive function F'(N) of a specific type corresponding to the given variant of basic data. This function, according to the assigned level of damage unacceptable to the attacker, helps us to find the value of deterrence index $P(N \geq N_{ud})$. The task of this approach is to provide estimates of a series of alternative variables of basic data in order to select the optimal one.

What is a basic data variant? It is a particular grouping of components and characteristics of the elements under study. We have described them earlier – nuclear delivery systems; their system of command, control and communication (C^3); global information systems. Each element, i.e., its composition and characteristics, contributes something to the overall result, changing its value in this or that direction. Concretely, it changes the value of probability $P(N \geq N_{ud})$ with a fixed value N_{ud}.

One of the major goals of this study is to determine the influence of changes in the above-mentioned elements upon the total final result. What is the contribution made by each one of them? Which element, or which component of an element, is the most important one? If we simultaneously estimate respective expenditures for introduced changes, we will arrive at the well-known cost effectiveness criterion.

Our approach has a very important peculiarity: it adds the aspect of *sufficiency* to the classical cost-benefit analysis in order to select the optimal variant.

Let us assume that we have analyzed a number of variables on the basis of index $P(N \geq 50)$, in which the composition and characteristics of the C^3 system change, while data for nuclear weapons and global information systems remain constant. The result is below:

C^3 Variables	Expenditures (conditional units)	Deterrence Index $P(N \geq 50)$
1	0.5	0.4
2	1.2	0.65
3	2.7	0.8
4	4.8	0.95

Table 3: Alternatives of deterrence effectiveness.

Which variable to select? Earlier it was believed, but unspoken, that the more the better, as far as effectiveness goes. Money was also taken into consideration. The "truth" was sought in the balance of these two categories.

Indeed, when it comes to estimating the effectiveness of our actions in a *really possible* (acceptable) war, the probability of victory should be as great as possible. The only limiting factor would be money (or resources in general). A hypothetical *world nuclear war* is an altogether different story, and should not be approached in the old,

traditional ways. It is recognized that there can be no winners in such a war, and this is our assumption.

Is not our mission to guarantee the destruction of the opponent? And if we are to guarantee this, what exactly does it mean? A guarantee may be viewed in terms of the magnitude of damage. For instance, it is a well-founded belief that 50 warheads delivered on target constitute unacceptable damage. But what about the second component of the degree of risk – the probability of retaliation?

It seems that if this component should guarantee destruction as well, then its value should also be infinitely approaching 1, as it would be in the above-mentioned case of conventional war. Then, even variant 4 in our example might not be sufficient, while the difficulty of achieving this index at the level of 0.999, under conditions of enemy counteractions, would be extreme. One could spend unimaginable amounts of resources without achieving these "nines."

Is this a dead-end? Yes, if our mission is retaliation *guaranteed to destroy* the opponent. But there is no dead-end if the mission instead is *guaranteed deterrence.* By the way, the latter goal is logically derived from the universally recognized general concept of strategic security and stability.

Still, skeptics may object: are we taking a conscious risk *not* to be able to retaliate in the case of an attack? To a certain degree this is so, but it is more useful to say that we are proposing to take account of reality. Moreover, we are not defining this borderline in quantitative terms, but only proposing a method to open up the real picture.

An approach taking into account the deterrent effect of risk allows us to hope for the establishment of realistic, and at the same time robust, levels of weapons, C^3 systems and information systems. For instance, according to our table, the potential attacker is not likely to start a war even in variant 1, because the 0.4 probability of unacceptable damage is quite impressive.

There may be great potential for lowering the reasonable threshold of deterrence. After all, the theoretical probability of an *unacceptable* event should equal zero! This is worth thinking about. However, we are not going to determine the value of this probability yet, especially since it is linked to the value N_{ud} – that is, to unacceptable damage. We are still addressing the issue of methodology.

Thus, reasonable sufficiency is added to traditional cost-effectiveness when estimating alternative variables. Here is an opportunity to make a quantitative estimate of this criterion according not to weapons potential, but to the forecast result. The abstract concept of probability becomes quite substantial, and can be evaluated by concrete expenditures. With the help of this concept, we can broaden our interpretation of the cost-effectiveness criterion, which might now be referred to more accurately as the sufficiency-cost criterion.

Our analysis may run in the following way. Variant 2 provides for deterrence, i.e., it solves the final problem, and requires expenditures of 1.2 conditional units. However, if we want to increase the margin of reliability for deterrence, and have the resources to

do so, we can implement variants 3 and even 4. At the same time, even with a shortage of resources, it would be considered risky to use variant 1 with expenditures smaller than in variant 2.

It is obvious that the variables should include several combinations among the components and characteristics not only of C^3 systems, but also of global information systems and nuclear weapons themselves. This would allow for a better balancing of cost-effectiveness between them. This in turn is quite important for developing a better substantiated, more sober policy for reducing strategic nuclear forces.

To sum this section up, the statistical imitation model investigates the ability of nuclear delivery systems, C^3 systems and global information systems as a whole to retaliate in response to a nuclear attack. After *k* wars, we obtain a distributive function for the random result of retaliation, and determine the value of a deterrence index for the given variant $P(N \geq N_{ud})$. This index is useful for comparing a number of variables embodying different components and characteristics for the whole object of study. Selection of the optimal variable is carried out according to a sufficiency-cost analysis.

3.4 The Command and Control System's Influence Upon the Final Result

We have already noted that the C^3 system has a decisive influence on the probabilistic distribution of the final result. We will examine the mechanism of this influence and attempt to find out why the C^3 system creates such a large point dispersal.

Let us look in some detail at the C^3 system as one element of our study, considering only those aspects that are important for answering our question. Fig. 8 is a diagram of the C^3 system within the framework of our research as a whole.

The separate components can be understood as follows:

Early Warning System (EWS) – the missile attack warning system, including communications channels to decision-makers, as well as the connected systems that produce information on the enemy's missile attack.

National Command Authority (NCA) – the organs and command posts of those military and political leaders authorized to make decisions on the use of nuclear weapons under specific conditions. This component also includes a special communication system for the leadership, and the system for communicating decisions to the command posts of the General Staff.

Command Posts of the General Staff and NCA (HLMCP) – The system of headquarters command posts that are authorized to issue orders to use nuclear weapons.

SINA – the system for identifying a nuclear attack, including sensors for registering nuclear explosions on home territory, summarizing this information, and communicating it to NCA and HLMCP.

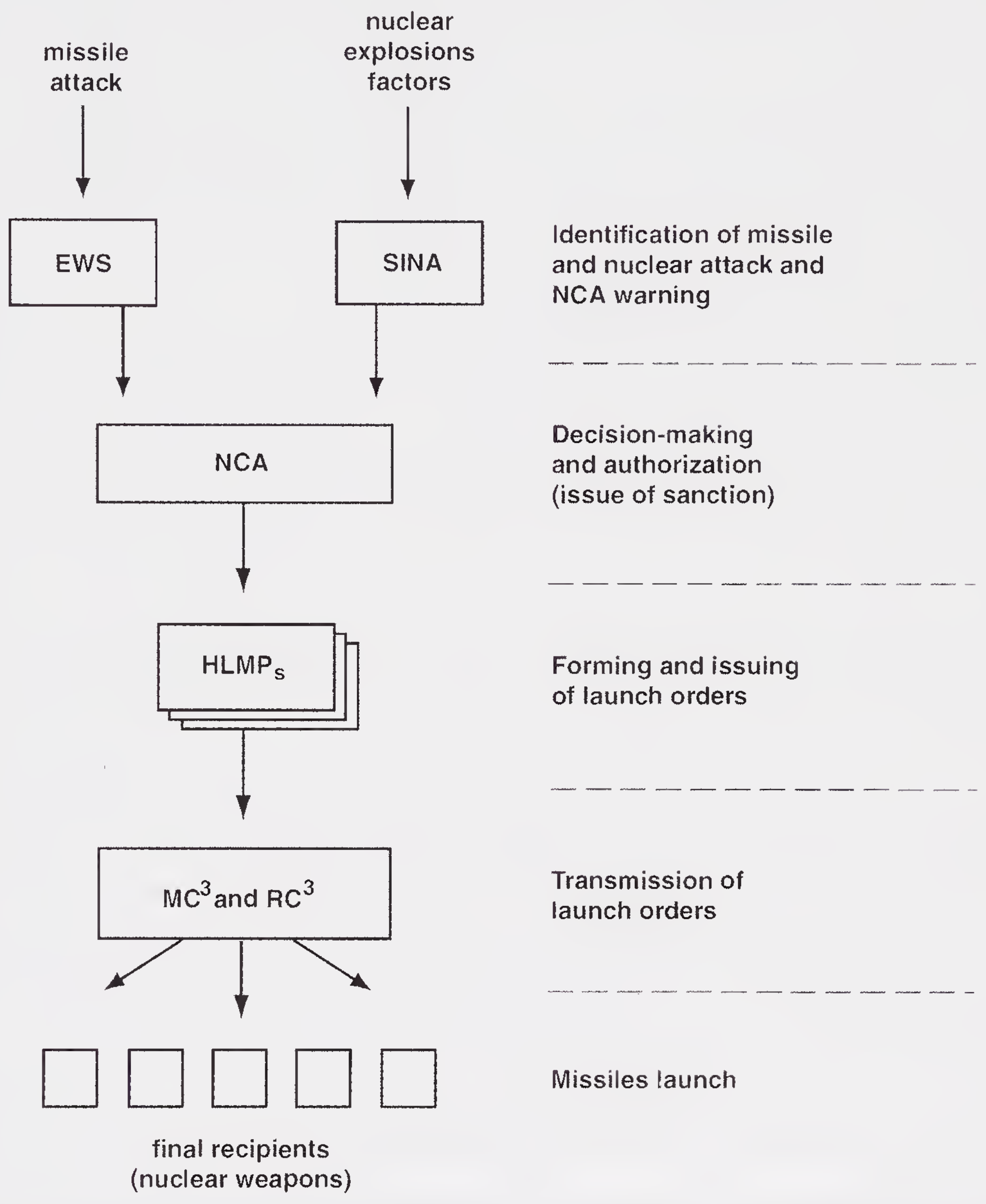


Fig. 8: Launch function of C^3 system.

MC^3 and RC^3 – the main and back-up command and control systems including communications centers, translators, and the communications lines between them and to the executing links. The fact that the MC^3 and RC^3 are presented as one component emphasizes that they are always used together for both launch-on-warning and launch-under-attack by the strategic nuclear forces.

Final recipients – the nuclear weapon delivery systems.

Generally speaking, we can further broaden the parameters of the command and control system by including the global information system (GIS). This is frequently and justifiably done.

In this case, however, we will not broaden our view, but will concentrate on the peculiarities of command and control systems in a more specific, narrow aspect. We will limit ourselves by discussing the question of the GIS' coexistence with command and control: first of all, in what form should the initial data from the GIS system be presented as it enters the command and control system?

Here are some clarifications for the flow-chart above:

In analyzing the problem of nuclear deterrence, we must emphasize the command and control system's primary function: to deliver launch orders to the nuclear weapons delivery systems, since strategic nuclear retaliation is carried out through this very function. This does not mean that while designing the system and estimating its cost, other functions should not be considered in evaluating the command and control system's functions. The following two statements should serve as starting points.

First, we assume that only those functions that may be utilized in the course of the system's operation, up to fulfilling its main objective – providing for massive retaliation with nuclear weapons – should be considered. These include all the functions that support effective deterrence, such as providing for the necessary degree of war readiness in the command and control system, and strategic nuclear forces as a whole, during peacetime. They maintain the established system parameters: primarily, stability during conventional military actions, with the goal of supporting the system's permanent readiness to fulfill its primary task. They also include the system's ability to provide selective nuclear strikes during limited nuclear conflict. And, finally, the most important function is to fulfill, if need be, the main goal of massive retaliation.

The time has come to look more critically at the advisability of planning those functions of command and control and nuclear forces as a whole, that are outside the framework of deterrence; that is, conducting subsequent strikes, etc. No one believes any longer that such actions would be possible under the conditions of a global nuclear conflict. For this reason, we will talk only about those functions providing deterrence.

Second, we will concentrate on just one main function – guaranteeing a retaliatory strike. We will work under the assumption that all studied variants of the command and control system differ only in the levels of their effectiveness for implementation of this main function; the rest of the functions we will assume to be fixed. We will certainly evaluate all of them when working out cost estimates, but we will pay special attention to the cost differences between the variants resulting from changes to the effectiveness of the main function.

Now it is necessary to briefly review the command and control system's mechanism for realizing this function. Some people may be justified in asking: "Aren't we going too far?" This is, after all, the "holy of holies," that which people used to be afraid even to mention! It would help to clarify this aspect of the question.

It is true that the command and control of strategic nuclear forces has remained for a long time one of the most classified topics. Even after practically all secrets about the weapons themselves (numbers, types, locations, etc.) had been revealed, command and control was hardly mentioned. The explanation is simple: there was no need, no "demand." But once the specific question of nuclear forces reduction arose, the parties were able to agree to open their most "holy of holies." The question became what to reveal. We will talk about this issue in more detail when discussing the problem of initial data. Here we will just mention one thing: it is ridiculous to conceal what is already known to everyone – the general design principles of command and control systems, for example, which are the same everywhere. Nobody, on the other hand, is going to reveal what is harder for the opposing side to learn: the location of mobile units, working frequencies, number of communication channels, unblocking codes for nuclear forces, etc. More detail on that further. Here, let us discuss the fulfillment of the command and control system's main function; that is, the launching of missiles. This is no secret at all.

A country's military and political leadership (the "leadership") [see Fig. 8] is a strictly defined group of people authorized by law to decide on the retaliatory use of nuclear weapons under extreme conditions. They are an integral component of the command and control system. No matter where these people are at the moment of a nuclear attack, they have to communicate with each other by "teleconferencing," and make a joint decision. A special communication system serves this purpose. After the decision is made, the leadership's authorization, numerically encoded, is passed along to those high level command posts (HLMCP) that can produce launch orders for nuclear weapons delivery vehicles. The HLMCP's crews would not be able to produce those orders without the presence of at least one of two conditions: receipt of the leadership's authorization, or the presence of a definite aggregate of factors confirming an enemy's nuclear attack.

We already discussed how that authorization is achieved. The second condition arises independently from the actions of the leadership, and is the command and control system's fallback "insurance" in case the leadership pathway does not work, for whatever reason. What are the factors fulfilling that second condition? They are a combination of data from the SINA, the complete disappearance of any communication channels with the leadership, and initial permission received from the leadership authorizing independent actions in such a situation (preauthorization). The presence of this combination of factors at a surviving HLMCP would allow the command post computations to produce and deliver a launch order to the delivery vehicles.

In any case, no nuclear weapons unit would be able to carry out its task of launching its missiles without receiving an order with the code for unblocking the weapons. This rigid centralization of the command and control system, and the potential for its being decapitated, are the main reasons why retaliation could have zero results.

How can this be?

Don't panic yet. Instead, ask yourselves two questions: is it possible to exclude this outcome completely, and do we need to exclude it? The answers will follow. Remain patient and we will continue.

More "exotic" variations in the design of command and control systems exist in theory. The so-called "dead hand" variant is an example. In this case, each nuclear weapons carrier is able to launch on its own upon "positive" identification of a nuclear attack. The word "positive" is not set in quotes for nothing. The question of removing the "nuclear monster" from human control is a special problem. Even if both sides reach an agreement that permits both of them to have such technology, allegedly for more "reliable deterrence," it does not change the essence of the approach we are considering. The initial data change, but the character of the results will not change significantly. The route defined by authorization (the first arm) remains intact under this variant, and "zero" results may almost disappear. But is this worth such a risk? Hardly. As of today, the two-branch system with authorization arriving from above remains a "classical" realistic variant. This will be the object of our further analysis.

Designing nuclear weapons command and control systems according to the "two-branch" variant has a deep strategic meaning. If we keep only the authorization route, we make our leadership hostage in a way. All results of this decision, unique in the history of humankind, will fall entirely on their heads. And they will be making this choice under extreme conditions, with severely limited time, and base it, in reality, only on technologically produced data from a warning system. The question of whether EWS data may be trusted is directly related to the problem of limiting nuclear retaliation. Such a situation will always tempt the aggressor to "take a risk," to try to overcome the only barrier wholly dependent on the human element. This situation is, obviously, hugely destabilizing.

This is why it is logical to have something like a second deterrence barrier that does not depend quite so much on human beings, because it is hard not to "notice" a nuclear war! If the first branch reacts to a warning, the second one reacts to the fact.

Sometimes, that part of the command and control system that initiates a reaction according to the C^3 warning is called the main system – MC^3, and the second part (second branch) – reserve system (RC^3). This separation is strictly abstract since both systems always operate together. RC^3 components are simply much more stable relevant to nuclear war, unlike the MC^3, whose main purpose is to authorize orders before any nuclear explosions take place. We will here speak of the system as a whole and will use the terms MC^3/RC^3 only as necessary, for convenient presentation of the material.

Thus, the presence of two branches within the system makes it more stable from the viewpoint of deterring a potential aggressor. Those two branches, however, differ according to the magnitude of retaliation they provide. The first branch allows participation of more nuclear weapons units in a nuclear strike than the second, since the latter's response is delayed until after nuclear strikes have begun.

At this point we can directly examine the influence command and control systems

have on the types of final distribution. Broadly speaking, three characteristics of this distribution are already obvious.

The first are of retaliation levels – namely the N_{wh} values – is the ideal performance of the command and control system, in which the authorization route (first branch) is utilized. In this case, the majority of nuclear weapon units will fulfill their task of launching the missiles even before the enemy's weapons hit. Such a strike is called, as we already know, LOW. The values of N_{wh} are highest in this case; for the most part, they will be affected by previous losses during a conventional war, as well as the effectiveness of the enemy's BMD. Let us note that this area has a rather small range of dispersal.

Let us analyze a quantitative example. Assume that the initial number of warheads at all units on the defending side was 6,000. Assume also that 2,000 of them had been destroyed in the course of a conventional conflict and 4,000 were intact at the moment of nuclear attack. We are assuming that during the LOW, the command and control system was able to employ all 4,000 of them. And, finally, let the enemy's BMD possess 50 percent effectiveness. Thus, about 2,000 warheads will reach their targets. Taking into account a certain number of random values, we can say our area of values is about 1,900 to 2,100.

The second probable area of values N_{wh} arises when the system didn't have time to work by the authorization pathway, but was only able to react to the fact of nuclear explosions on home territory. Such a nuclear strike is called LUA. It is clear that the values of N_{wh} here are lower than for LOW. But by how much? It depends on the time factor: how fast the command and control system reacts on one side, and how fast the number of nuclear weapon units will "vanish" under enemy nuclear attacks.

It is worth noting that the timing of an enemy's nuclear hits, as part of a mass strike, may be somewhat protracted. According to the most popular model, a simultaneous launch of all its missiles is most preferable for the aggressor. In that case, the first warheads from its submarines might reach home territory within 12 to 13 minutes, and the last – from the North American continent, say – only after 30 to 35 minutes. Thus, we can talk about an approximately 20 minute span for a nuclear attack. This is the working interval by which the reaction of the command and control system, according to its second "branch," should be analyzed. Further on, we will look at some peculiarities of command and control performance within this interval. For now, we will just make note of a much greater range of values for N: 500-1,500 for our example.

And the third area is that of null outcomes. In this case, the command and control system has not performed through either of its "branches," no order to unblock nuclear weapons has been issued, and no nuclear warhead has been launched. This is the scenario in which the enemy succeeds in "beheading" the command and control system. It used to be that everybody kept quiet about those "nulls," yet, we cannot get away from them. And let this area occupy its legitimate position in our general picture.

If we combine all three areas, we will get a picture of the probable distribution for the final result, shown in Fig. 9:

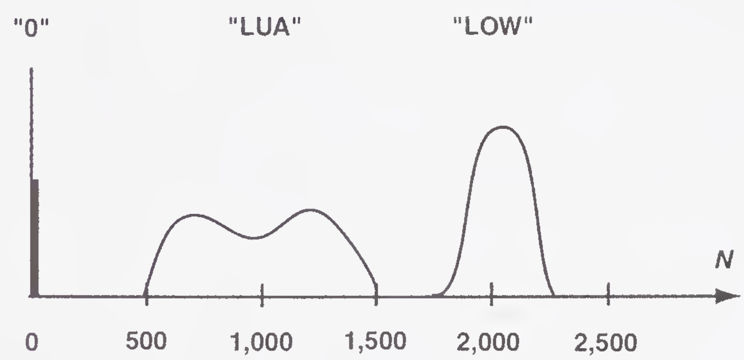


Fig. 9: Combined picture of all possible results of modelling.

All three areas discussed are quite probable. The only realistic "sample" (that is, a nuclear conflict) may produce any N_{wh} value from the discussed areas. Which one? Nobody will ever say, nor is able to say. The complete lack of certainty is a deterring factor here. At the same time this probabilistic picture contains another type of crucial information – costs. It is from the relationship between the opponents' forces – that is, relative costs – on which the specific type of distribution depends. The number of null outcomes, high volume strikes, or mediocre results depends on relative costs. Knowing the value of unacceptable damage N_{ud}, we may then establish the value of the deterrence indicators – $P(N \geq N_{ud})$.

This is, generally speaking, the mechanism by which the command and control system influences the final distribution. Now we can go farther and look at this influence's characteristics in some detail.

Fig. 10 illustrates four variants of the command and control system. "Command and control system operability" can be separated into two components: the actual time it takes to deliver an order from the center to the executive units (t), and the delay before transmitting the order begins, that is, the system's "reaction time" (t_{del}), where *del* is *delay*. CS will stand for Command System.

Let us assume that in the CS-1 and CS-2 variants the actual delivery time is much less than the length of the enemy's nuclear attack: the system performs immediately. But in the CS-1 variant, the response of the system is higher than in CS-2. For example, in CS-1 the order was delivered prior to the enemy's nuclear attack. In that case, the character of the final distribution is determined mostly by the preliminary impact of conventional weapons and the effectiveness of the enemy's BMD. At that, the distribution law is close to normal, and the final indicator $P(N \geq N_{ud}) \sim 1$.

In the CS-2 variant the order is delivered only during the enemy's nuclear attack; consequently, a portion of the missiles is not launched and gets destroyed. The distribution moves to the left by the value of the delay. Yet the distribution type remains normal, because the τ is low. The final result is $P(N \geq N_{ud}) < 1.0$.

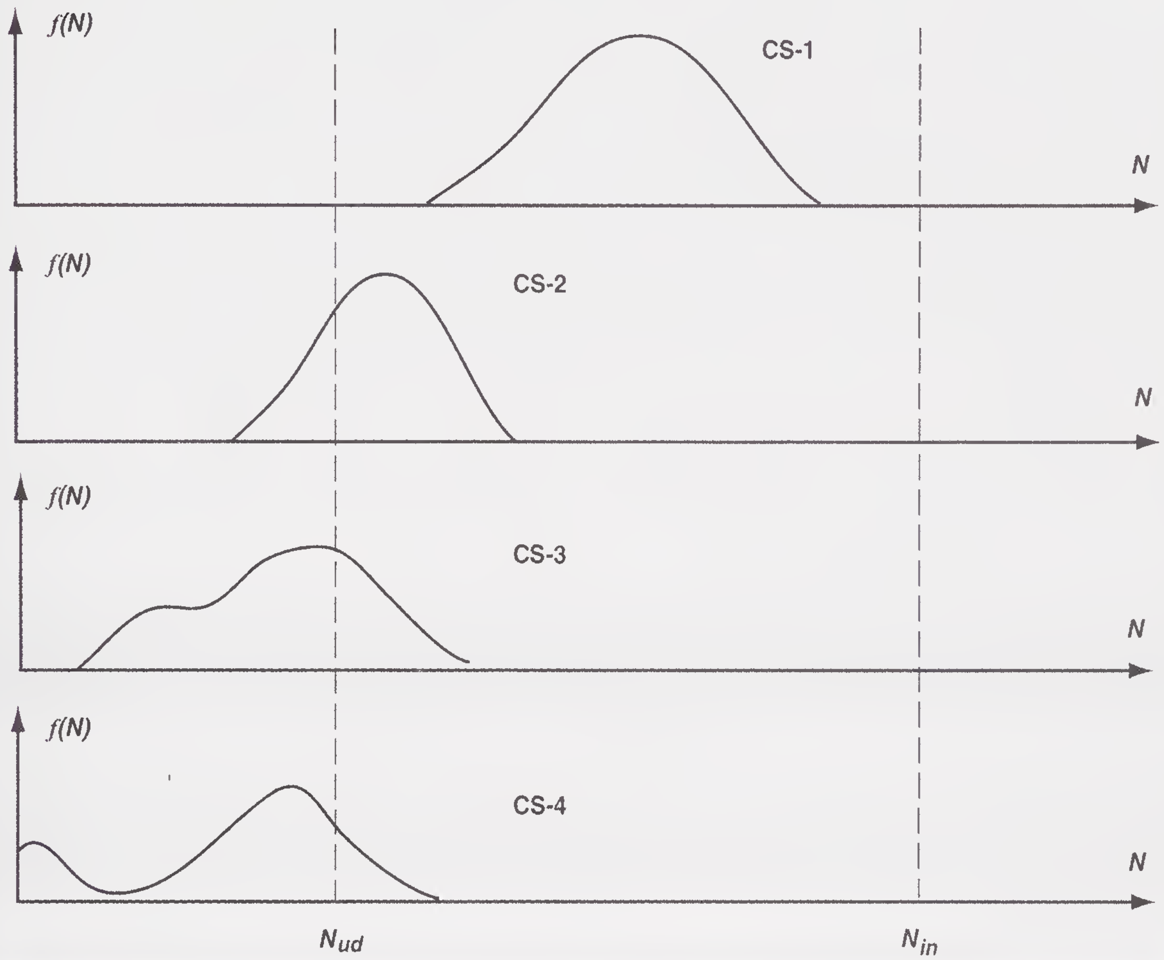


Fig. 10: Influence of CS type on form of distribution density of results.

In reality, however, it is extremely difficult to design a command and control system that would work instantaneously while under attack by an enemy. Its subsystems vary in the speeds with which they deliver information, and in their vulnerabilities. In a nuclear war the influence of these factors is, naturally, random in character, resulting in a distribution that is stretched to the left. When the system is improved (CS-3) the final result is higher; when it is less efficient, it is lower (CS-4). As noted earlier, null outcomes remain a possibility. The probability of these (even when low) is determined by the level of rigid centralization in nuclear command and control systems.

From Fig. 11, it is obviously important to consider another command and control characteristic, the so-called "regime of saturation."

As shown in the drawing to the left, strengthening the command and control system improves the final result only up to a certain point. "Saturation" appears in this graph, which is, in reality, a cohesion graph. The value of this limit is determined by factors outside the system of command and control, mostly N_{in} and BMD effectiveness. In the

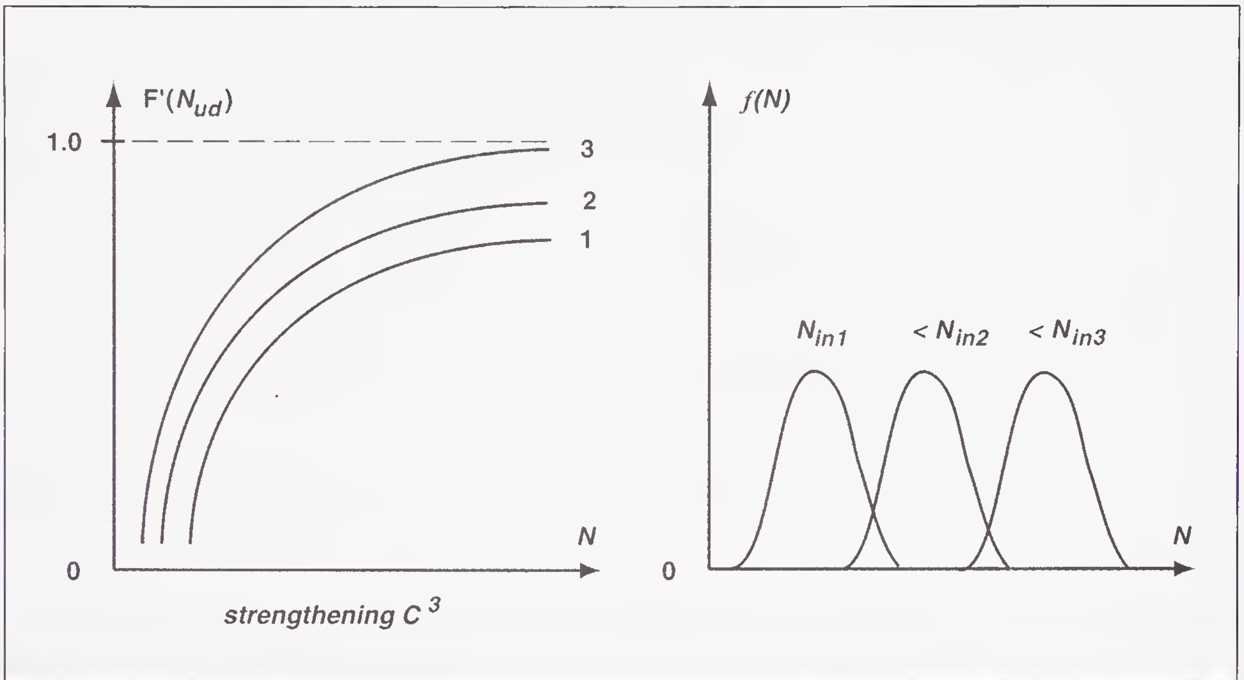


Fig. 11: Saturation of C^3 systems.

above drawing on the right, we see the most saturated C^3 system possible under various N_{in} and with fixed BMD effectiveness. In previous drawings, the CS-1 and CS-2 variants implied a "saturated" command and control system; in CS-3 and 4, a non-saturated one.

A study of the command and control system's effectiveness in executing its main purpose – launching nuclear weapons (that is, with the use of the distributive function F'(N) – suggests a possible interesting direction in streamlining the structure of the system as regards necessary sufficiency. In Fig. 12, we can see a simplified command and control structure. MC is a major, or general, channel from the source (center) to the "distributor." IC is an accounting, or individual, channel from the "distributor" to each receiver (nuclear weapons carrier). The study questioned the interdependence between the character of the final distribution and probabilistic – temporary characteristics of the MC and IC channels. Simulation showed that the final distribution depends on them significantly.

Fig. 13 demonstrates the distributive function for the three variants of the C^3 structure. Variant 1 presupposes high (close to maximally achievable) characteristics for both MC and IC. The final result is close to 1 over all the considered stretch of N. Curve 2 describes the variant where the MC remains on the same level, but the IC characteristics are much lower. Variant 3 is the opposite of variant 2. Which is better?

If level $F'(N)_3$ is sufficient for nuclear deterrence, then all variants are the same under low N_{ud} (i.e. $N_{ud\,1}$), even though the first one is more expensive. If N_{ud} is increased, variant 2 may be found unacceptable. A comparison between variants 1 and 3 favors the latter, since it costs less with the same acceptable result. This conclusion is demon-

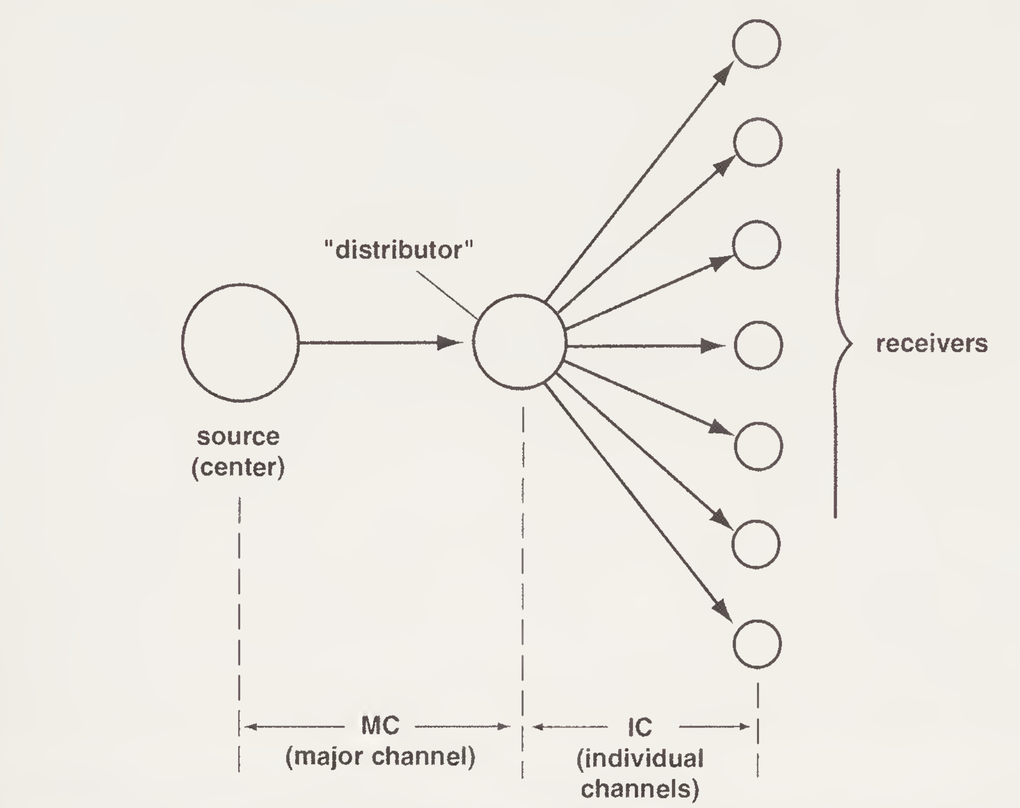


Fig. 12: Simplified structure of command system.

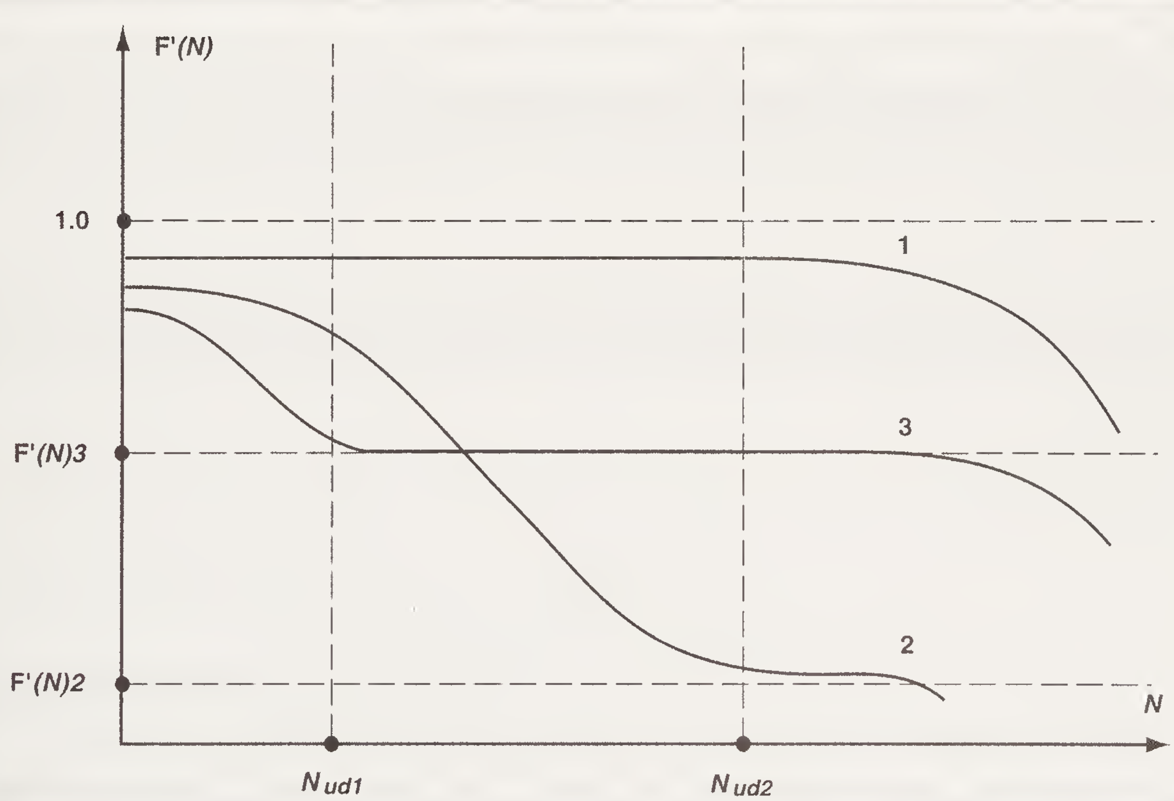


Fig. 13: Distributive function for three variants of C³ structure.

strated visually on the flow charts of the distribution density f(N) correlating to the considered distributive functions. (See Fig. 14)

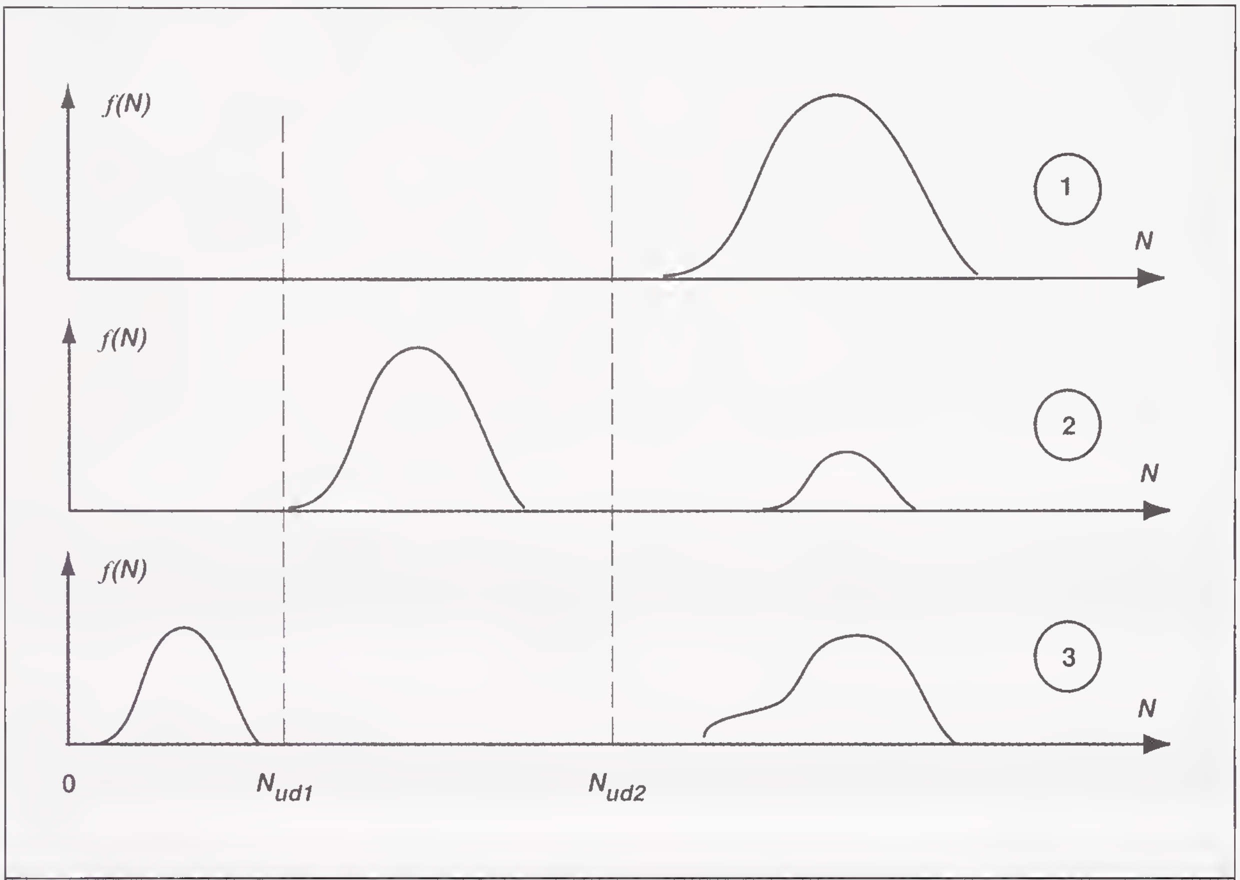


Fig. 14: Distribution densities for same CS structures which are shown in Fig. 13.

Since the immediate "source" is a part of the major channel, we may pose this question: what is preferable – a system of command posts or the network for data delivery? In the search for a reasonable level of sufficiency, the channels appear to be more important. Simply speaking, the individual channels mostly define the number of units participating in the strike (within the framework of the N_{in} level and BMD parameters), while the command posts and major channels in general define the probability of them reaching their targets (the "luster effect"). It is better to have a minimally acceptable probability of the required damage level than a higher probability of insufficient damage. Specific conditions should certainly be considered, yet general consideration of the noted dependency may be of practical value.

These particular characteristics of the command and control system strongly influence the final result, and are crucial for further analysis.

Summarizing everything discussed here, it is important to note that the command and control system has a greater impact on the final result than any other factor. This is because of the rigid correlation between groupings of nuclear weapons carriers and

the C^3 system. The system guides the carriers the way a conductor conducts a choir. He is able to include everyone, single out the basses and tenors, or make everyone silent, all at once.

It is important to remember that this correlation is not carried out exclusively on the highest level – issuing or not issuing the launch order. Subsystems that are part of the general configuration and deal with large groups of carriers of various types, also make a difference. Therefore, if any such subsystem fails, the final value of retaliation is changed. As a result of this, the statistical distribution may have a multimode character. For example, let us demonstrate a few such probable types of distribution for the different variants of the command and control system (Fig. 15).

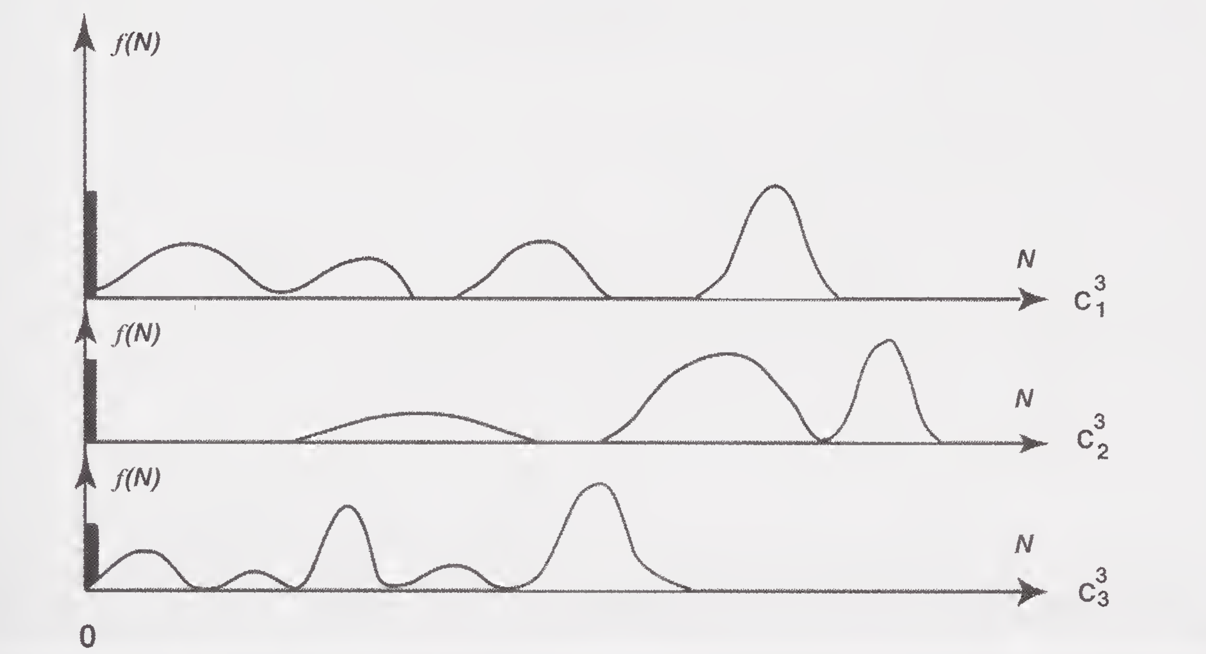


Fig. 15: Possible types of distribution density for variants of CS structure.

Such charts are not at all in conflict with the earlier statements on the three areas of the N values. The areas of LOW and "0" remain intact, while the LUA area may consist of several separate "fragments." All those details are determined statistically, according to the results of repeated simulations.

3.5 Practical Aspects of the Method

In this part, we are going to review various aspects of the suggested method that characterize its practical value. We will try to draw some conclusions with its help, and clarify a number of methodological questions. The final goal of this review is to decide whether this method has a future, and is worthwhile to continue developing and implementing.

3.5.1 Influence of Certain Factors Upon Final Distribution

We saw in sufficient detail the influence of the command and control system's characteristic on the type of final distribution. Let us remember now that those characteristics consist, in their turn, of two factors – the system's own technical parameters and the degree of the enemy's effect on the system's components.

It is now useful to look at how the final picture depends on two more important components of the initial data – the initial general number of nuclear warheads (N_{in}) and the amount this number is reduced by the enemy's conventional and nuclear attacks (Fig. 16); and the effectiveness of the enemy's BMD in reducing the number of nuclear warheads that reach their targets (Fig. 17).

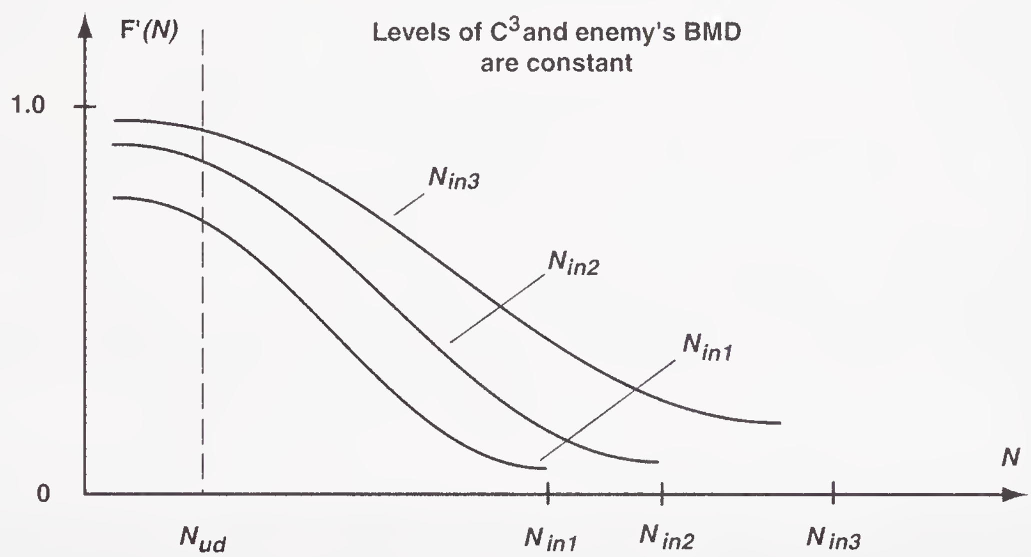


Fig. 16: Influence of N_{in} on distribution function.

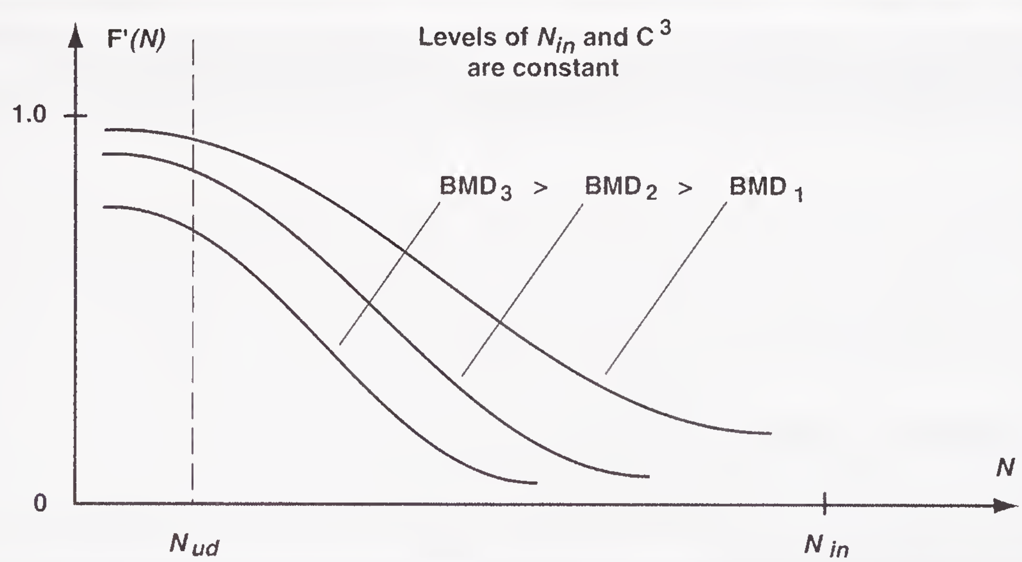


Fig. 17: Influence of BMD systems on distribution function.

When the levels of C^3 and the enemy's BMD are constant, the greater initial potential of the strategic nuclear forces, the higher the final result, i.e. effectiveness of deterrence. Let us note that, at a high initial N, it is easier to create a command and control system that is needed for achieving the required results.

The more effective the enemy's BMD, the lower (when N_{in} and C^3 are constant) is the probability of achieving the desired result of nuclear forces retaliatory actions. It is also clear that if the N_{in} is higher in the figure above, the curves will go higher.

3.5.2 On the Distributive Function and Mathematical Expectation

Many works in this area have used mathematical expectation (m) as the main indicator of effectiveness. It is, however, well known from the probability theory that the distributive function provides a fuller description of a random value than mathematical expectation. This analysis demonstrated very clearly that this is especially true while studying problems of sufficiency.

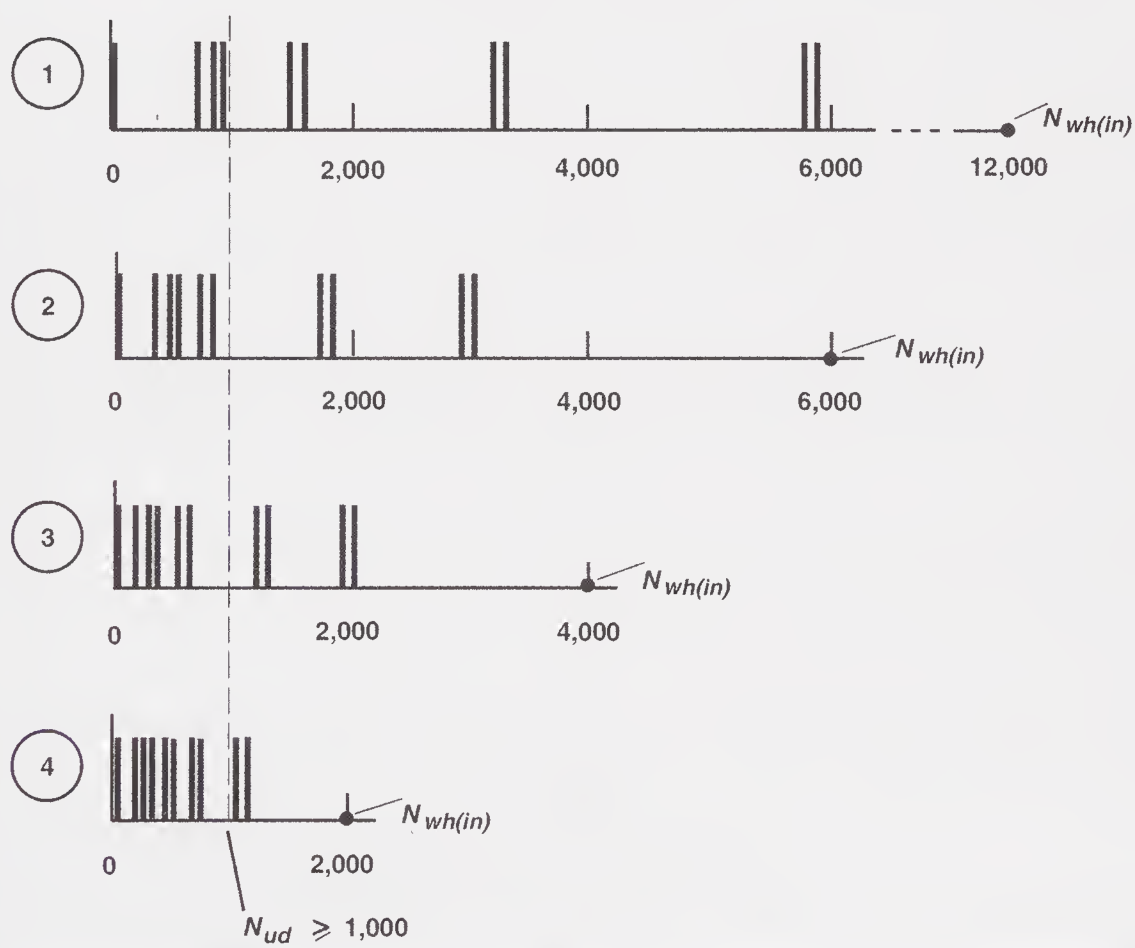


Fig. 18: Comparison between mathematical expectation *(m)* and deterrence index $P(N \geq N_{ud})$: clarity of estimation of possible results of retaliation.

Let us compare the conclusions that may be drawn on the basis of conditional initial data by applying *m* and F'(N). To make it more graphic, we will review discrete distributions for only 10 realizations on a statistical model. Equivalents of those distributions with the use of real initial data and the required number of simulations do exist. (Fig. 18)

No	N_{in}	*m*	$F'(N_{ud})$	Comments
1	12,000 (100%)	2,500	0.6	*m* is much greater than N_{ud}. But $P(N \geq N_{ud})$ is only 0.6, that is quite below 1.0.
2	6,000 (50%)	1,250	0.4	With *m* close to N_{ud}, probability of $P(N \geq m)$ may be below 0.5, the distribution law differs from the norm.
3	4,000 (33%)	830	0.4	*m* is already lower than the required level N_{ud}(=1,000), while probability $P(N \geq N_{ud})$ remains unchanged at 0.4.
4	2,000 (17%)	420	0.2	*m* is substantially smaller than N_{ud}, while the value of $P(N_{ud})$ can be considered sufficient for deterrence.

From the table it is clear that using F'(N) provides more information than *m*. For example, even when *m* is considerably higher than N_{ud}, the probability of unacceptable damage is still far from 1. Also, while *m* changes over a wide range (from 1,250 to 830) the value of $F'(N_{ud})$ remains unchanged (0.4). Speaking of sufficiency, the table demonstrates the following: when using *m*, the allowable reduction in the initial number of nuclear units is 50 percent; further reduction is impossible since *m* is less than N_{ud}. The conclusion is somewhat different when applying the distributive function: the 33 percent level also proves acceptable; as for the 17 percent level, everything depends on our attitude to the value of $P(N \geq N_{ud}) = 0.2$. If this is a sufficient deterring factor (this is, after all, the probability of unacceptable damage!), then such a level of reduction is also acceptable. This cannot be seen when using only *m*.

The difference in the amount of information between using *m* or F'(N) is even more obvious when considering extreme situations. (Fig. 19)

In the top drawing, the result is zero in eight out of 10 simulations, while in the two other cases it equals 5,000 warheads. Mathematical expectations = 1,000. In the lower drawing, with a different control and command system, zero result appears only in one simulation, while in nine cases 1,000 to 1,100 warheads reached their targets. Mathematical expectation is still about 1,000. But there is a huge difference in the $F'(N_{ud})$ indicator: 0.2 in the first scenario and about 0.9 in the second one. The physical characteristics of the two compared command and control systems are very concrete; therefore, the study of the distributive function is crucial.

Of course, mathematical expectation can certainly be used as an additional indicator

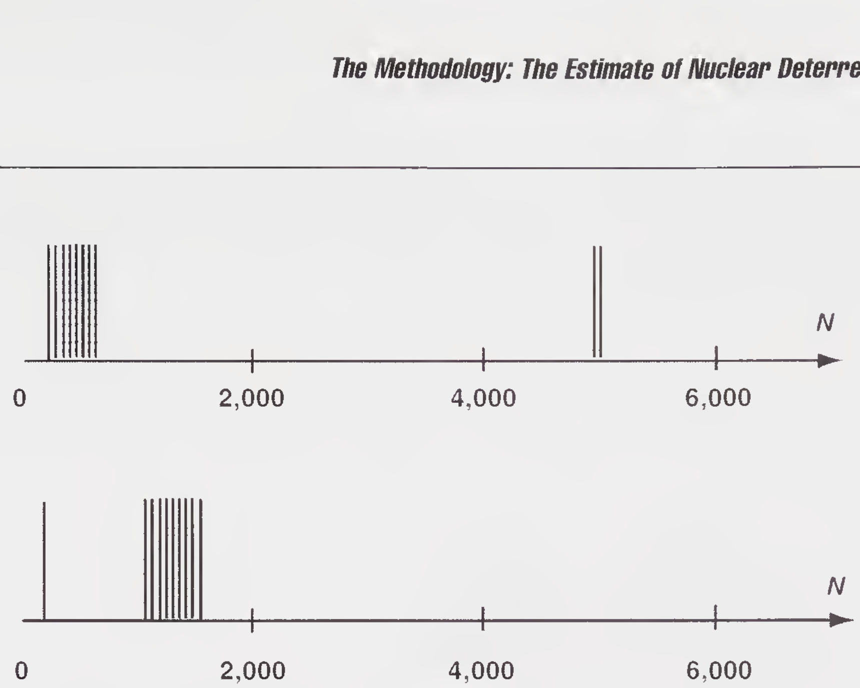


Fig. 19: Extreme cases of differences between *m* and P(N≥N_{ud}) from the point of view of information content.

for general orientation. It may be noted along with dispersion, etc. Having stated, however, that "m = 1,250," we have to clarify whether this is a little or a lot. It is much easier to state, without any additional absolute values, that the probability of unacceptable damage is 0.4.

How precise is such an estimate? Everything depends on the correct tallying (accounting) of transition points in discrete distribution. It would be useful to provide that range of values. For example, for variant 1, we may say that P(N≥950÷1,050) = 0.6, and for variant 4, P(N≥900÷1,000) = 0.2. As a whole, as usual, precise estimates depend on the precision of the initial data when using either m or F'(N).

Let us also remember that if m signifies a "point" (average point), then F'(N) is an area. F'(N_{ud}) means the probability of all numbers higher than N_{ud}, i.e. P(N≥N_{ud}). In our example for variant 1, those values are 1500, 3,600, and 6,000 warheads. All these values are unacceptable for the enemy. At the same time, with the help of F'(N) we are able to characterize all the "left area," i. e., for the values N< N_{ud} down to zero. For example, in that very same variant 1 it follows that P(N≥800) = 0.9 and, accordingly, P(N = 0) = 0.1. This is of no small importance for an all-purpose evaluation of the sufficiency problem.

3.5.3 Reduction of Strategic Nuclear Forces and Sufficiency

Let us try to review this complex and multifaceted problem using the approach outlined above, and with the understanding that this is only one aspect of a broad problem.

Fig. 20 clarifies the essence of the method of estimating the admissible reduction of nuclear force levels while guaranteeing effective deterrence. We assume that the levels of enemy BMD and the command and control system are constant. In this case, when

consistently reducing the initial potential of strategic nuclear forces (N_{in}), the probability of unacceptable damage to the enemy is reduced. Naturally, the prospects for both sides to develop conventional and nuclear weapons, BMD, etc. should be taken in consideration whenever possible.

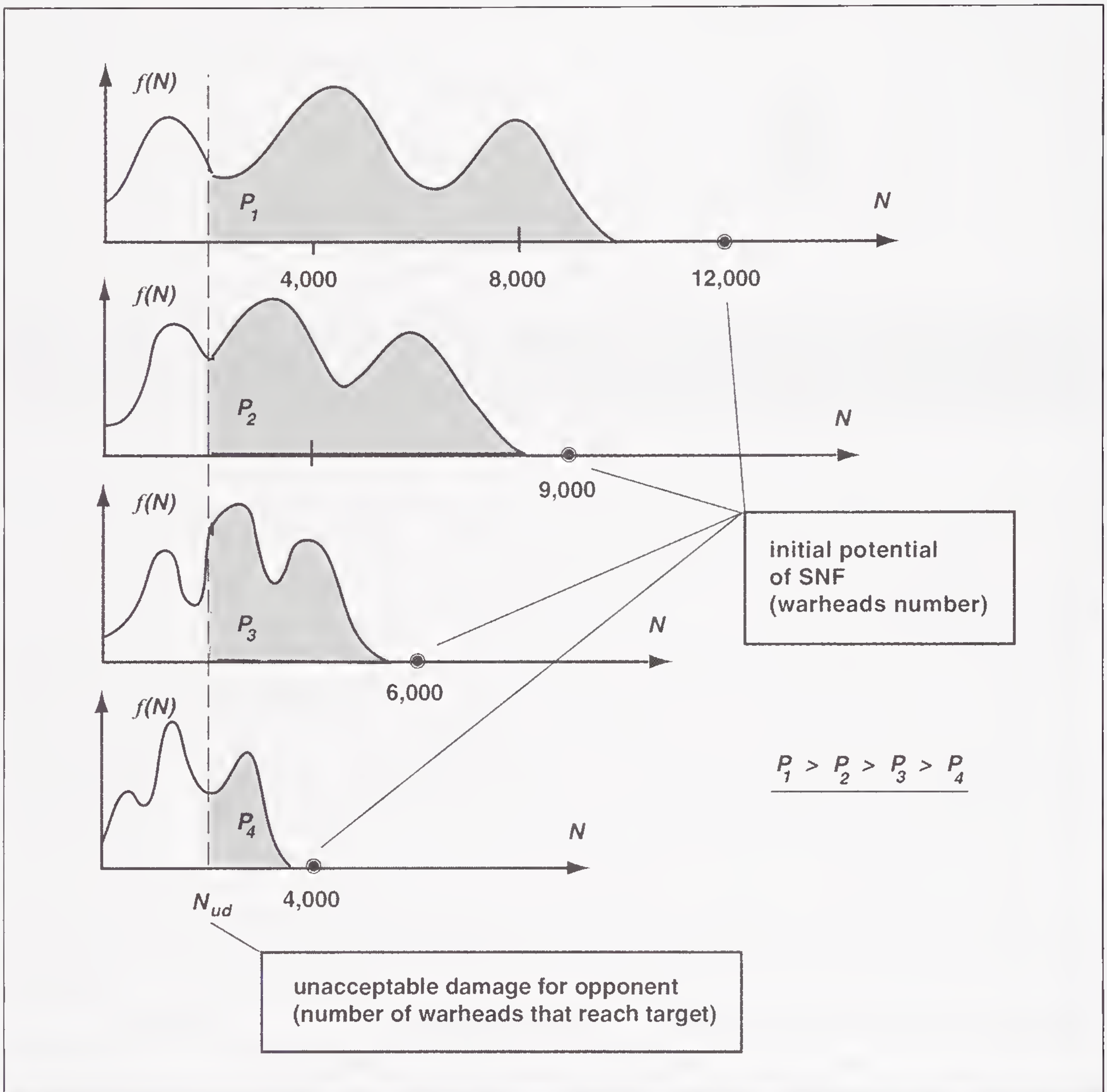


Fig. 20: Influence of nuclear arms reduction on value of deterrence index $P(N \geq N_{ud})$.

Down to what probability value and what level of damage should we reduce? This is a very complicated question, embracing all aspects: military, political, and philosophical. The question of damage levels is a key problem for nuclear disarmament and is being intensely studied. The goal of this chapter is to demonstrate that we cannot limit ourselves to researching only damage levels. Accounting for the probability of those

levels is necessary; in this case, the concept of a deterring factor acquires a fuller, different meaning. This is even truer because each increase in probability costs substantial amounts of money.

3.5.4 Sufficiency and the Criterion of Cost Effectiveness

The greatest significance of the economic aspect of deterrence lies in the huge investments put into strategic nuclear forces. A crucial question arises: what is the relationship between the savings from strategic force reductions and the cost of maintaining a deterrence potential even at the minimum necessary level?

Here, too, we should mention the important contribution of the command and control system. First of all, the defensive character of our military doctrine requires the speedy creation of a command and control system that can provide effective deterrence even if our strategic nuclear forces have to carry out a delayed retaliatory strike. Secondly, on top of those "initial" expenses, the command and control system demands long term investments in order for it to compensate for any reduction in deterrence as a result of general strategic force reductions. Costs for developing command and control systems are quite comparable with savings through general nuclear force reductions, since they will be, for the most part, costs for operating existing weapons only.

The following Fig. 21 shows one of the possible relationships between savings and expenditures, and should clarify certain peculiarities:

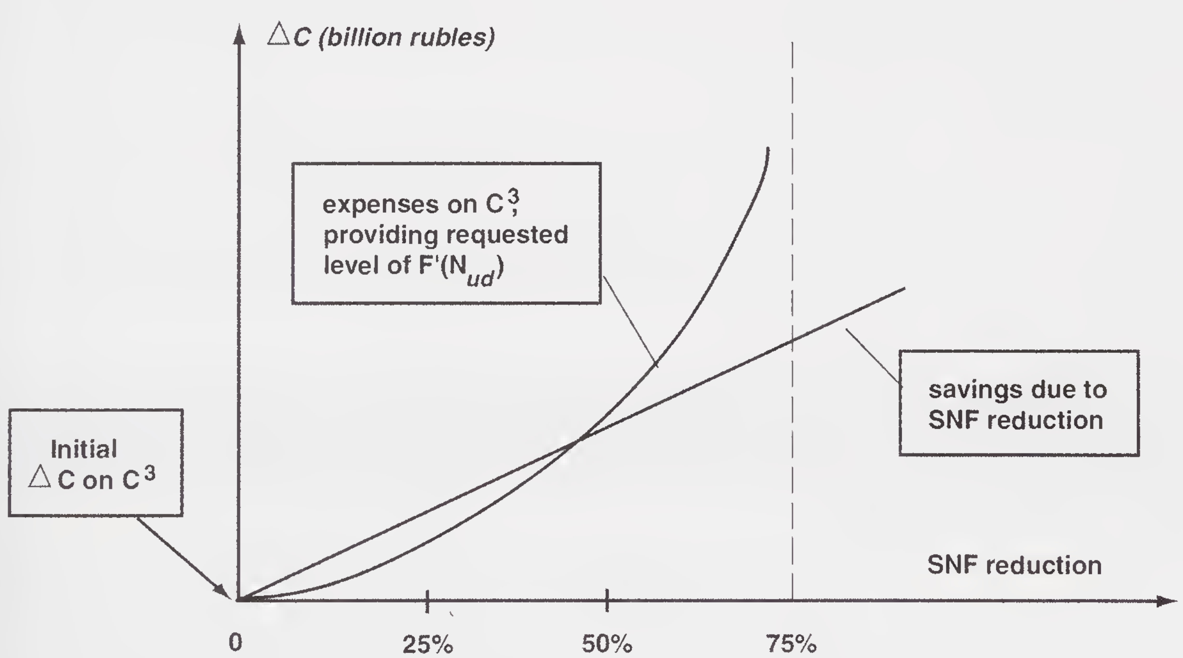


Fig. 21: Correlation between expenses on C³ and savings due to SNF reduction.

On the X axis we can see the degree of reduction in present day levels of strategic nuclear forces; on the Y axis, we find costs or savings. With a 75 percent nuclear force

reduction and an established value for the main effectiveness indicator F'(N), we reach the limit beyond which any increase in spending for the command and control system does not result in an increased F'(N) (the saturation/regime of C^3). If we reduce nuclear forces down to 50 percent, C^3 expenses may be lower than the savings on the nuclear strategic forces themselves. This is the favorable area from the point of view of savings. In the area between 50 percent and 75 percent force reduction, C^3 expenses exceed savings; the deeper the reduction, the faster this difference grows. The optimal parameter should be located in this latter area – the boundary beyond which additional expenses will not be justified by strategic force reductions.

It is clear from previous chapters that if a different, lower value of $F'(N_{ud})$ is established, or the value of N_{ud} itself is reduced, then the savings will allow deeper reductions in nuclear forces (more than 75 percent).

3.5.5 Possibility of an Asymmetrical Decision

Analyzing the problem of sufficiency with the use of the F'(N) indicator allows a new approach to the question of asymmetry. As is known, this problem is caused by differences in conditions, primarily geographical, for the nuclear forces of the United States and Russia. In the United States, those conditions are more favorable, especially for both weapons and command and control systems.

When estimating equivalent initial nuclear potentials, it seems that the final result, i.e. the damage, may be different. To phrase it more correctly, the differences will not be in the damage itself, but in the probabilities of the same damage levels for both sides. For example, if N_{ud} is the same, for one side $P(N \geq N_{ud}) = 0.6$, while for the other side it is only 0.4.

But such degrees of risk may be as unacceptable for both sides as may be 0.5, and 0.3, etc. Everything depends on the established deterrence parameter. Thus, it appears that up to a certain level of equal reduction, asymmetry need not be considered at all. And this minimal level of equivalent reduction may be lower than when orienting ourselves only to the damage level.

Later, either asymmetrical reductions in strategic forces or reductions in the levels of N_{ud} and $P(N \geq N_{ud})$ as agreed by the parties will, of course, become necessary.

3.5.6 The Area of Stability

Since the command and control system plays such a crucial part in nuclear deterrence, it would be interesting to consider how the strength of countermeasures against it would be reflected in the final result. Is it possible to totally suppress the system, so that the probability of the aggressor's side receiving excessive damage will not be higher than acceptable? Calculations have demonstrated that this is a challenging task.

The graphs (Fig. 22) show the possible changes in the value of $F'(N_{ud})$ under the influence of increased ratio of expenses for an attack against the command and control system (C_a), and expenses for protecting it (C_p). Thus, on the X axis the ratio is C_a/C_p.

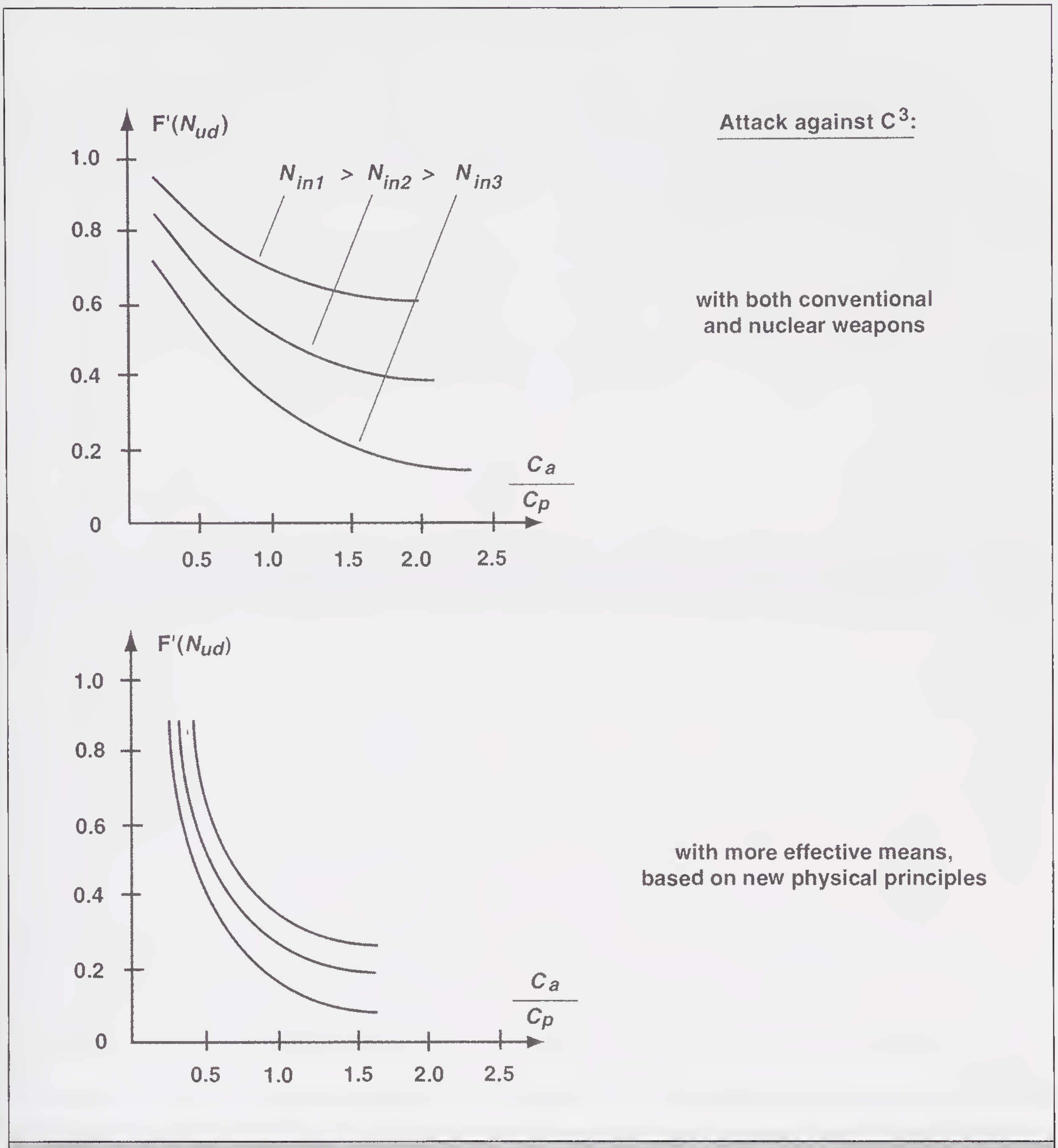


Fig. 22: Influence of ratio between expenses for attack against C^3 system (C_a) and expenses for C^3 protection (C_p) on distribution function of retaliation results.

From the charts it is obvious that the dependence of the final result on the value of the relationship C_a to C_p is a non-linear one. On the lower levels of F'(N) the "effect of small numbers" manifests itself, which means that, using measures against the command and control system, it is much harder to reduce the final result from 0.2 to 0.1 than from 0.7 to 0.6. This is equivalent to the well known principle of the possibility of creating reliable systems from sufficient numbers of less reliable components. In the same way, it is hard for the defending side to maintain F'(N) on a very high level: for

example, to maintain it within the parameters 0.90-0.95, the defender has to invest more in maintaining the system than the aggressor in its suppression.

Yet, as noted earlier, the whole point is that very high levels of F'(N) are not needed to maintain reliable deterrence. And under lower levels of this indicator, the correlation of expenses becomes favorable for the defender; the lower this level, the higher the difference in those expenses.

Summing it all up, we should mention the potential presence of a certain stability (a reserve of reliability) when asymmetrical (lesser) efforts by the defender will, for practical purposes, neutralize the aggressor's much higher expenses, thus maintaining the threat of a final result that would be unacceptable for the aggressor.

Adjusting the upper limit of the stability area is made possible by establishing a corresponding value for the initial potential of strategic nuclear forces (N_{in}). The higher the N_{in}, the higher the level at which it is possible to achieve this upper boundary.

The upper chart in Fig. 22 shows interdependencies under conditions when the adversaries use both conventional and nuclear weapons. The lower chart shows a situation in which the opponents use more effective weapons based on new physical principles. Precise estimated values are only achievable with sufficiently reliable initial data; it seems, however, that the essence of existing interdependencies will remain.

If those areas of stability are realistically achievable (considering the economic potential of each side), this factor may be of considerable practical importance. In this case, allocating sufficient means for complete suppression of the command and control system makes no sense; this may lead, in its turn, to changes in strategy in which most resources are used to destroy weapon systems themselves, primarily nuclear weapons. The goal of such a strategy would be to achieve the same result without attacking the command and control system, but concentrating instead on reducing the enemy's weapons' potential below the level of unacceptable damage. It is approximately the same as the transition from curve 3 to curve 2 in the drawing illustrating the rational structure of the command and control system (Fig. 23). Curve 3 favors the defender; curve 2 is more favorable for the aggressor.

Today a significant portion of resources is intended for suppressing command and control systems. This, and the fact that the strategies and levels of weapons on both sides are now subject to negotiations, make the above considerations quite important. Further studies on this question would serve a good purpose.

3.5.7 Transformation of the F'(N) Function into an F'(W) Function

Up to this point we have been using the F(N) type distributive function, where N is the number of warheads reaching their targets on the aggressor nation's territory. This parameter is widely used in most studies and we will continue using it. Sometimes, however, it is useful to introduce another concept – the damage to the enemy. We will code it as the letter W. Since W is also a random value, we will be talking about the distributive function of F'(W). One needs to know how to change from one function to another.

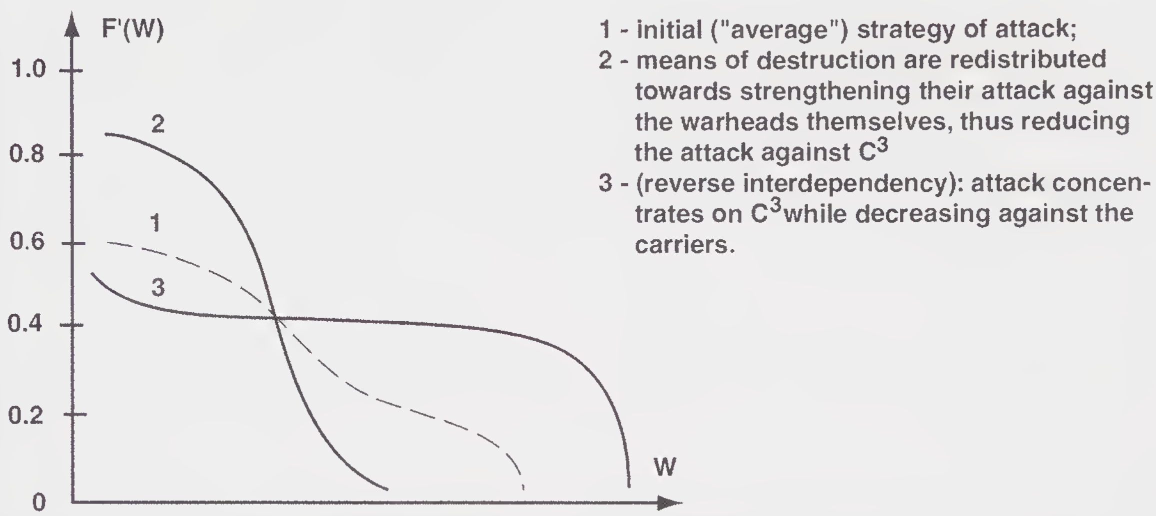


Fig. 23: Influence of attack strategy on the form of F'(W) function.

Among various interpretations of "damage," the one most useful for our purposes is to select a general indicator W, which is expressed in the percentage of the enemy's conditional integrated potential. Then the process of switching from F'(N) to F'(W) appears to be rather uncomplicated. It consists of the following steps. For each simulation of nuclear war, a group of warheads that have fulfilled their mission appears. Each of these warheads is assigned in advance to a specific target in the battle plan for using strategic nuclear forces. During each simulation, it is possible to establish the magnitude of damage by analyzing the "successful" warheads (that reached their targets). Then, summing up all simulations, we can arrive at F'(W).

This method is applicable if the damage W is expressed by one indicator: a percentage of the initial potential. But the damage may also be represented by several indicators that include its various aspects – military, industrial, social, environmental, etc. There is a method available for this situation also. When analyzing each simulation in the model, the sum of "successful" warheads (destroyed targets), provides a "yes-no" type of answer. Upon completing our simulations, instead of the distributive function we use a $P(W \geq W_{req})$ type point evaluation. W_{req} is interpreted as an integral estimate of damage according to all the indicators.

For the sake of convenience, we will be using both types of distributive functions F'(N) and F'(W), depending on the material.

3.5.8 Rationalizing the Enemy's Strategy

It is not necessary to go into a detailed explanation of how important it is, when simulating, to select the enemy's most rational strategy of attack against the opponent's nuclear weapons carriers, the command and control system, and the GIS, in order to

reach a reliable estimate of the final outcome.

We start with the initial assumption that a potential aggressor who is planning a nuclear strike will address the problem of distributing all his military potential (conventional, nuclear, radio-electronic warfare) between existing targets. In any case, we know that his means of attack are limited (especially his nuclear weapons).

The approach presented here allows for rather flexible prognoses of potential solutions to the aggressor's problem. Since we have selected $P(N \geq N_{ud})$ or $P(W \geq W_{ud})$ as common indicators for all nuclear retaliatory actions, it would be logical to use the same indicators to select rational strategies for the opponent's planned attack.

To simplify our argument, let us assume that all the elements of the GIS are part of the command and control system. (See Fig. 23) Thus we will be able to view the opponent's problem as the need to distribute his means of destruction between two types of targets – nuclear weapons carriers and the command and control system.

Curve 1 is the initial ("average") strategy of attack. Curve 2 reflects the changes when the means of destruction are redistributed towards strengthening their attack against the warheads themselves, thus weakening the attack against the command and control system. Here the level of potential damage is reduced but its probability increases (the curve moves upwards to the left). Curve 3 is the reverse interdependency, in which the brunt of attack is against the command and control system while fewer weapons are targeted against the carriers. In this case, the curve moves down to the right, that is, the level of potential damage increases, but its probability decreases.

The goal of each side's strategies may be to "maintain" the curve of the forecasted final outcome in that area favorable for it. (Fig. 24)

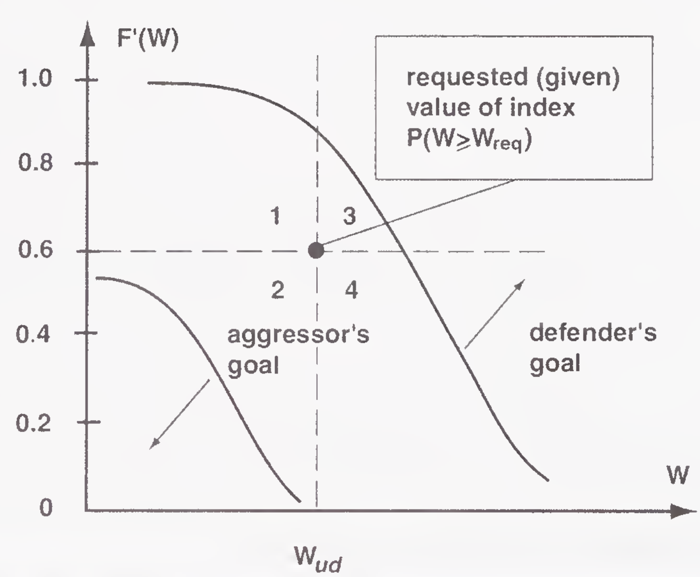


Fig. 24: Goals of strategies of sides.

The point where two perpendicular lines cross is the value of the indicator $P(W \geq W_{ud})$ sufficient for achieving the goal of deterrence. The above mentioned lines form four areas. Area 2 is the most acceptable for the opponent if he is the aggressor. His strategic goal is to keep the entire curve of the distributive function F'(W) within this area. The arrow signifies the enemy's effort to reduce the effectiveness of our retaliation to zero. Our strategy's goal is to see that the curve F'(W) goes through area 3, that is, exceeds the deterrence parameter.

During peacetime confrontation, variants in which neither goal is achieved are also possible. Those are shown in Fig. 24.

Fig. 25 illustrates a case in which the enemy, unable to keep the curve F'(W) in area 2 only, plans the distribution of his offensive assets in such a way that the curve remains in areas 1 and 2. If the enemy is still going to risk an attack, his strategy in this case may be metaphorically called the strategy of "costly victory." This means the opponent deliberately selects a high probability of damage, but at some level lower than unacceptable.

The opponent may choose a different strategy, if he has limited capabilities. The right section of Fig. 25 shows a distribution of offensive weapons in which the curve F'(W) goes through areas 2 and 4. In this case it is impossible to exclude damage values that are greater than unacceptable, but the probability is relatively low. We may call this "a strategy with the risk of annihilation."

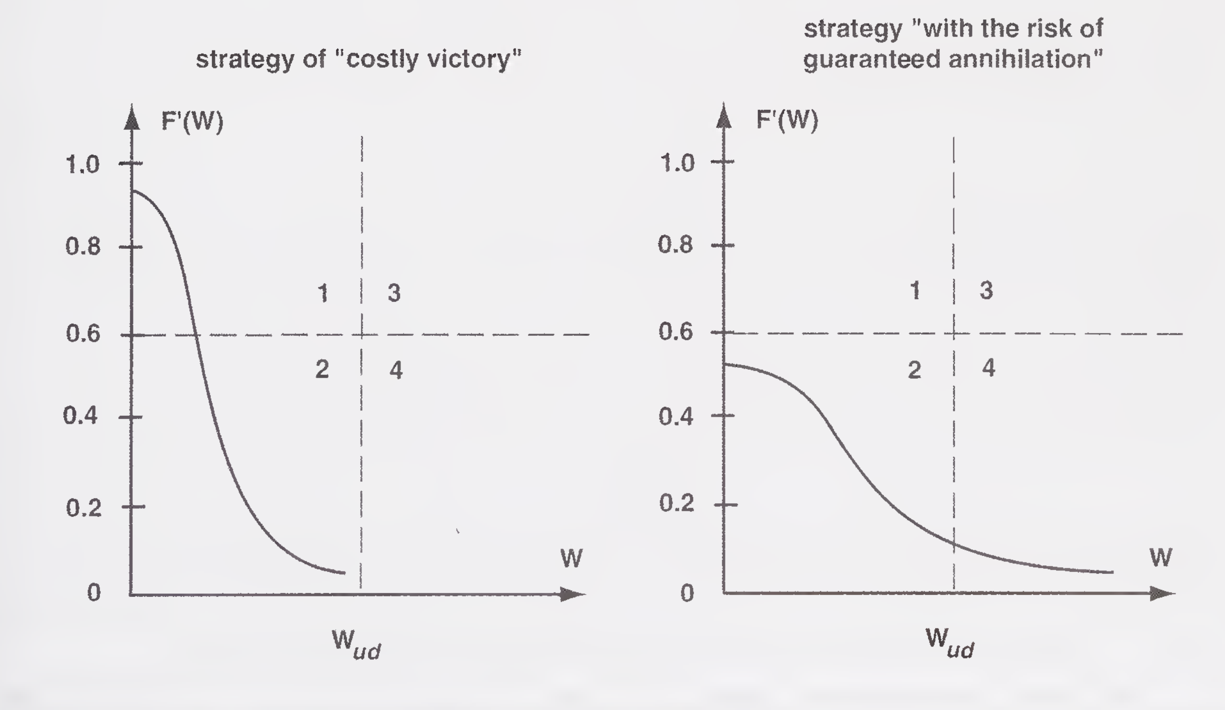


Fig. 25: Intermediate (non-optimal) strategies of attacker.

The lower the levels of W and P are, the higher the temptation to start nuclear aggression under the two latter strategies. We are unable to predict which of the two extremes the enemy would select if he risks an attack. From our point of view, therefore, it is not desirable to allow the use of either of the "unstable balance" versions discussed above. The only variant with a guarantee should be the one in which the curve F'(W) goes through three areas - 1, 3, and 4, with an expected damage level greater than unacceptable and a high probability. Let us remember that establishing a sufficient value for $P(W \geq W_{ud})$ is a special question which is not considered in this work.

This method for rationalizing the enemy's strategies allows us to realistically evaluate in advance the current relationship between the different sides' forces during peacetime. It may be that we are already in a state of unstable balance because the temptation is sufficiently high for a potential aggressor (if, for example, the distributive function is only in area 2 or goes through 1-2, 2-4). This is hardly a situation with which anyone can be satisfied, and something should be done. Curve F'(W) should be "forced" into area 3. How do we achieve that? There are many ways: reduce the enemy's impact; do not rush with the reduction of N_{in}; or perhaps review together the value of the deterrence indicator. That should be done both for N_{ud} and for the probability values. In any case something should be done, and the method suggested here may be of aid.

3.5.9 Independence of Analysis of the Command and Control System

When analyzing nuclear deterrence, purely military questions should be considered in close connection with all aspects of the threat, including the moral, social, ecological, and other indicators. This is an unavoidable condition, without which calculations make no sense.

It is important to note, however, that this condition is only relevant for establishing the *value* of unacceptable damage. In any case, once all threat factors have been gathered under this concept, in the end we ought to have a certain number of warheads, with certain characteristics and with an optimal plan for their use. This indicator is necessary in order to establish subsequently the required *probability* of delivering to their targets no fewer than that number of warheads. And this probability, as we saw before, is for the most part defined by the command and control system.

As for the command and control system itself, it may be analyzed separately from the combination of factors mentioned above, since they are going to be taken into account in the assigned level of unacceptable damage. This is what we understand as the independence of research on command and control system's sufficiency.

3.5.10 Forming Requirements for the Command and Control System

One of the most important practical aspects of the suggested approach is that it helps to define the contribution of one or another command and control subsystem (or a separate component) to the overall outcome. On this basis, it is then possible to assign

corresponding requirements for the system's characteristics. With that in mind, here are some general considerations for determining requirements to command and control systems.

As we have come to see, a command and control system is quite a complex and branched cohesion graph. It includes a series of subsystems (cable, space, radio, etc.) with various transmission speeds, stability under enemy attack, degrees to which it reaches the carriers, and other indicators. At the "end" of these systems are nuclear weapons carriers that also vary considerably in their survivability, numbers of warheads, etc.

It is clear that no matter how hard we try, we will not succeed in completely separating the command and control system and the weapons into two "autonomous" parts, at least not from the point of view of analysis and estimating results.

In principle, it is possible to separate them in this way: here is a specific missile, and here are the six command and control channels of various types connected to it. But here is a different carrier – an SSBN. It has a different number of warheads and, for example, four C^3 channels of a different type. And so on. It is impossible to bring all those varieties down to one standard.

Why are we even talking about separating the command and control systems from the weapons? Unfortunately, attempts to do so continue even today. Quite frequently, the picture is presented in an unacceptably primitive way: Here is a group of 6,000 warheads, from which about 3,000 survive by the time retaliation begins. Here is a command and control system that guarantees the delivery of orders to the nuclear weapons carriers with an "average" probability of 0.8. So, the fans of this approach reason that the final result will be on the level of 2,400 warheads.

Is this correct? Absolutely not! We have already seen that with the correct methodological approach even the character of the final result is different – it is a distribution, not a point.

Such complete averaging is certainly absurd. So is a more detailed averaging. For example, it is impossible to say that the probability of an order reaching the Strategic Rocket Forces units differs from the probability of its reaching SSBNs. The probabilities are, of course, different between the legs of the Strategic Nuclear Forces triad, but probabilities within each leg of the triad are also different. You have to consider the type of carrier, its location, the degree of the enemy's potential impact in the deployment area, etc.

But even this is not all. Within a specific subsystem of C^3, one must discuss the probability of delivering orders in just one geographical area with the greatest caution. One must not forget about the concepts of circularity and ensemble. Let us review this problem with the aid of a simple abstract example.

Let us assume we have a space command and control system, as presented in Fig. 26. An order from Earth (HMLCP) is passed along the major channel (MC) to a satellite (space apparatus SA) and from it, along individual channels (IC) in a circular fashion.

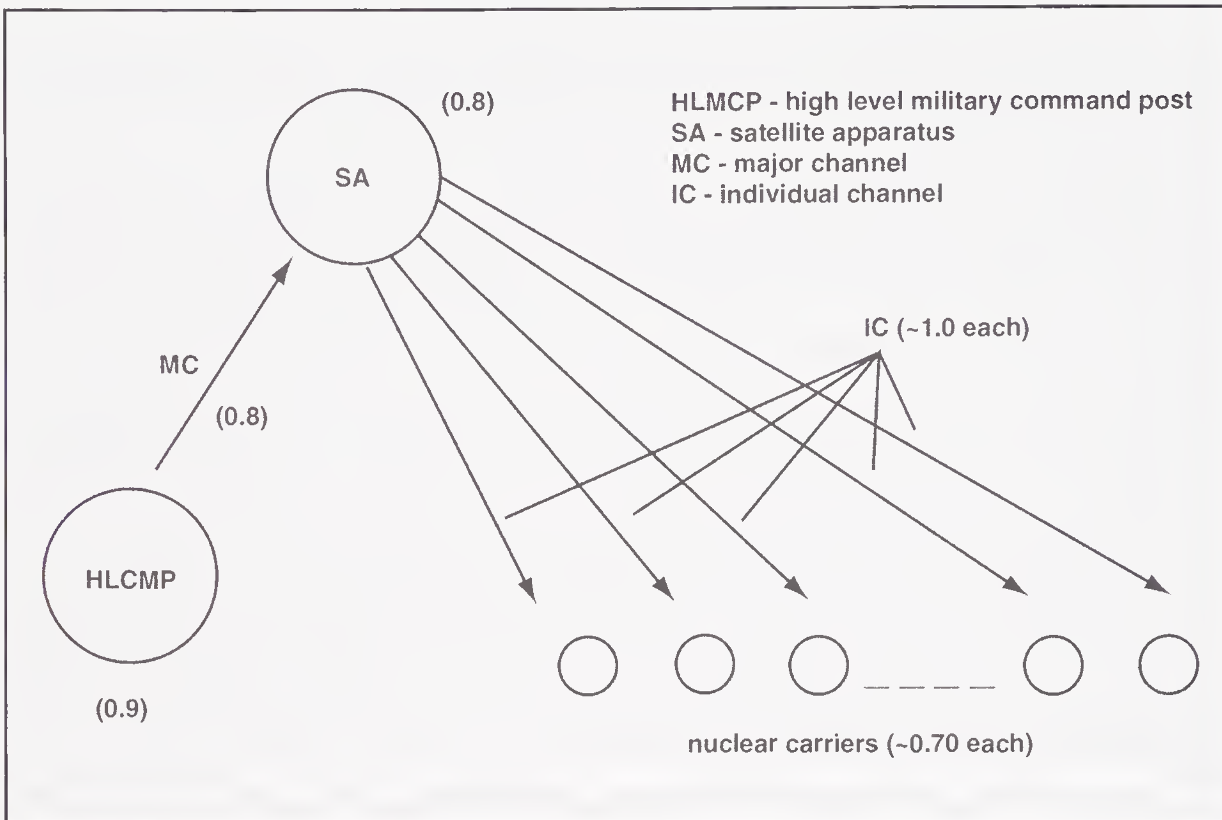


Fig. 26: "Circularity" and "ensemble."

An order from Earth (HMLCP) is passed along the major channel (MC) to a satellite (space apparatus - SA) and from it, along individual channels (IC) in a circular fashion to 100 identical nuclear weapons carriers, each of which has 10 warheads. Considering the enemy's attack, the probability of these elements functioning is: HLMCP = 0.9; MC = 0.8; SA = 0.8; carriers = 0.7 each. Let us assume the probability for IC to be about 1.0.

How do we evaluate this result analytically? Imagine we have a broom with a handle (HLMCP, MC, SA) and a brush or sweeper (IC).

First of all, by the time the order is delivered some delivery vehicles will have been destroyed. About 70 will still function, since 100 multiplied by 0.7 = 70. Altogether they will have only 700 warheads. Then we multiply probabilities for all parts of the broom's handle: 0.9 x 0.8 x 0.8 = 0.58. So, the probability of the handle's survival is approximately 0.6. So far everything has been correct. But from here, it is possible to select a right or a wrong way.

The wrong choice is to multiply the handle by the sweeper: 700 by 0.6 = 420. So, we've arrived to the already familiar point estimate: about 400 warheads should supposedly reach their targets.

In reality, though, using the correct approach gives a totally different answer: either 700 warheads reach their targets (the probability of this event is 0.6) or none do (probability is 0.4). And that's it.

These are the simplest, most elementary factors, but we have to be reminded about

them. We should not forget that in a real command and control system there will be many such interconnected "brooms." Such a network is hard to describe in an analytical way. The best result is the calculations provided by the statistical simulation model (SIM).

So, what is the correct approach to formulating requirements for the command and control system under these conditions?

It appears that the most correct way would be to estimate its effectiveness according to the final indicator $P(N \geq N_{req})$. This is a so-called "external" indicator of the effectiveness. This author thinks that only external indicators should be used for the command and control system *as a whole.*

Naturally, they should be applied with a concrete grouping of nuclear strategic weapons in mind. C^3 and nuclear weapons are organically inseparable, and the indicator $P(N \geq N_{req})$ is common for both of them.

Now, what to do with separate command and control subsystems, including newly developed ones? For instance, for the SRF. We may, of course, form our requirements for their contribution to the effectiveness of the SRF's retaliatory actions. It would be better, however, to review this contribution with the whole SNF in mind, that is, using the general model.

And, finally, how do we establish requirements for separate components (routes) within a subsystem? Here we are talking about "internal" effectiveness indicators; that is, the characteristics of the subsystem's components. In the example above, this means performance probabilities of the HLMCP, MC, SA, and IC. Requirements for them should be developed by breaking down the external indicator of the subsystem's effectiveness, and with consideration for each component's contribution and cost. And only after that, on the basis of the established requirements for the probability of performance, we can develop strictly technical requirements for each component. These requirements will be checked during the subsystem's testing. After they are specified and agreed upon during the tests, the final overall result may be elaborated with the help of the model.

This is how we see the "ideal" way to develop and establish requirements for the command and control system, which would allow for a more justified selection of priorities and planning of expenses.

From all of the above, it follows that it is theoretically incorrect to talk about the probability of delivering an order to the "ensemble" (SNF, SRF, etc.). Such a probability can be assigned only in relation to one addressee. And this can only be checked during testing. As for the command and control system as a whole, its effectiveness may be estimated only according to an external indicator. We suggest using the indicator $P(N \geq N_{req})$.

3.5.11 Miscellaneous

Let us introduce here some additional thoughts on the characteristics of the suggested approach.

This method permits us to approach an understanding of such a novel category as the minimal level of deterrence. It is important to emphasize that this will not be a fixed value. On the way to deep nuclear arms reductions, the use of the suggested generalized indicator $P(N \geq N_{ud})$ appears to be very convenient. During each new step toward reducing the deterrence threshold, each side may, by mutual consent, re-estimate both components of the indicator; that is, the values of unacceptable damage as well as of its probability.

This is a good time to clarify the concept of "guaranteed retaliation." We can certainly guarantee a certain damage value in advance, exceeding the unacceptable damage level with a considerable margin of safety. But the probability of such unacceptable damage in retaliatory strikes being equal to1.0 is theoretically unachievable. If this value approaches1.0, it excludes any opportunities for a strategic nuclear weapons reduction and requires additional astronomic expenditures for the command and control system. The principle of "the more the better," that was applied until recently, has no place if we are to resolve the problems of defense sufficiency. At the same time, "guaranteed deterrence" may be achieved by establishing rational values for the probability of unacceptable damage.

It is still too early to establish those acceptable levels of deterrence. It is necessary first to study all possible probable outcomes of a nuclear war, taking into account future weapons development and their costs.

It is interesting that unlike many ideas proposed today, this approach does not have any costs. This is because all we are talking about is an improvement in the evaluation system, making it more natural. Who said that the evaluation systems used before are perfect and that there are no other ways? If we change our approach, maybe the whole picture of strategic balance will look different. And savings, if there are any, could reach billions. It is probably worth trying.

It is also important to note that this method of evaluation is most applicable exactly to strategic nuclear weapons when the final result can be expressed using specific numerical values for damage, or for the number of warheads reaching their targets. For conventional weapons, the task of estimating a level of reasonable sufficiency is more challenging because of their widely varying uses, and the difficulty in selecting a generalized indicator of their effectiveness. It is possible that using the approach suggested here for conventional weapons might turn out to be useful as well.

This method has been considered from the standpoint of a "duel" between two sides, Russia and the United States. If necessary, however, it can be extrapolated to much a broader group, including all current and potential members of the nuclear club. After all, everything will be determined by the degree of risk to a potential aggressor.

One more consideration is very important for the problem of sufficiency. This method assumes an integrated approach to estimating the deterrence factor, for both LUA and LOW strikes by SNF. If estimates are done separately for LOW and LUA, a correspondingly high level of deterrence factor should be maintained. For example,

a problem in which no fewer than 500 warheads have to reach their targets should be resolved with the probability of 0.9 for LOW and 0.9 for LUA. If we do it in an integrated way as suggested here, in order to receive the general value of $P(N \geq 500) = 0.9$ it is, simply speaking, enough to have the $P_{low}(N \geq 500) = 0.7$ and $P_{lua}(N \geq 500) = 0.7$. This costs considerably less. Thus the margin of sufficiency is quite large.

And one last thing: the very character of deterrence moves us towards using it in a democratic way. Indeed, when we compare only nuclear potentials – how many submarines, planes, warheads, and missiles each side has – it looks quite abstract, like something only the military can understand, not ordinary people. But it is very different when the threat is expressed by a specific number of warheads "over your head," and with a certain probability of such an event actually happening. This is true especially if specific values of $P(N \geq N_{ud})$ are accompanied by real numbers for expenses. These are the expenses that come from the taxpayer's pocket. Here an ordinary citizen can see the scale and cost of his/her own fear. This cannot remain the business just of the military. On the basis of the suggested method, it is obvious that such decisions should be made by the entire society, represented by its democratic institutions.

3.6 Summary: Principles and Advantages of the Suggested Approach

We have reviewed the essence of the proposed approach to C^3 assessment, its main characteristics, and methods for its application. Although research is conducted in this field, there exists practically no summarized description of the method for a general audience. What follows is a summary of the method, including the method's principles and advantages, that should serve as a motivation for its further improvement and implementation.

This method of assessment can be used to establish quantitative levels of reasonable sufficiency for C^3 and strategic forces in general. It is based on the following principles:

- mutual deterrence is the basis of strategic stability;
- a potential aggressor is deterred by the risk of unacceptable damage through retaliation;
- the magnitude of the retaliatory damage is random and is greatly dispersed – from zero to corresponding maximal values;
- the type of distribution and the dispersion of the retaliatory damage random value depend partly on the characteristics of the potential victim's nuclear weapons forces, but especially on the characteristics of the target's command and control and global information systems;
- the risk to a potential aggressor is best expressed by the deterrence indicator, $P(N \geq N_{ud})$;
- a level of reasonable sufficiency for the potential victim is established by the condition that the risk to the potential aggressor is not lower than what he considers acceptable (assigned), that is $P(N \geq N_{ud}) \geq P_{ass}$;

- when using this indicator, we may substitute for the traditional criterion of "cost-effectiveness" the criterion of "cost-sufficiency." In this case, all spending above the level of "reasonable sufficiency" will increase the safety margin of robustness of deterrence;
- the sufficiency of C^3 and strategic nuclear forces as a whole is a stable concept, in that no matter how much the enemy spends on his SNF, the potential victim can always maintain the effectiveness of his SNF at a level sufficient for deterrence with the help of less expensive, asymmetrical measures.

The main advantage of this approach is that it may allow us to determine a quantitative substantiation for the concept of reasonable sufficiency. This refers not just to C^3, but to the whole complex of strategic nuclear forces, including groups of nuclear weapons carrier, global information systems and C^3. This approach to assessment can also point the way to a rational balance between all these parts of strategic nuclear forces, thus providing the required deterrence level with the minimum expenses.

Three areas in which reserves of sufficiency can be opened up with the use of this method should be pointed out:

1) An integrated assessment of the risks of both LOW and LUA. It is possible to obtain a required value for the deterrence indicator with relatively smaller indicators for LOW and LUA, which means reduction of general expenditures.

2) Limiting the missions of C^3 and accordingly, SNF as a whole, to deterrence of a potential aggressor.

3) Establishing the value of the deterrence indicator at a reasonably minimal level, by accepting, for example, $P(N \geq 1000_{wh}) = 0.8$ as a sufficient probability, rather than demanding the probability of 0.99. The 0.99 probability is unachievable from a technical and economic point of view, and is not even necessary for deterrence. (These numbers, however, are used merely as an example; we are not going to select them now.)

Even if these reserves do not result in big savings, and the calculated indicator of deterrence turns out to be "on the edge" or dangerously low, obtaining this kind of information can still be important for taking appropriate measures to prevent a nuclear war. It can point out some answers to broader questions, such as, what are the value and price of fear? And what is the real potential for a conflict?

This type of assessment may help bring about new thinking, and a better understanding of the concept of nuclear threat – that is, not only the scale of damage, but also its probability. In that case, the question of capabilities of nuclear weapons, GIS and C^3 needed for deterrence could be determined democratically by appropriate governmen-

tal committees, within parliaments, etc. The nuclear threat is a serious reality costing many billions of dollars.

Following is a list of practical tasks that can be accomplished using this new approach to force assessment:

1) assess existing C^3 systems according to indicators of effectiveness and sufficiency;

2) analyze the contribution of any specific new C^3 subsystem (being developed or introduced into use) to combat effectiveness of SNF;

3) evaluate the sufficiency of a program of C^3 development, and prioritize subsystems;

4) determine requirements for newly developed C^3 subsystems, based on an assigned level of a final outcome indicator (reverse task);

5) determine the most rational allotment of resources among various C^3 components, in order to provide a required final result;

6) develop practical recommendations for a sensible ratio between the levels of strategic nuclear forces, and of the C^3 system, keeping in mind "cost-effectiveness" criterion and various plans for SNF reduction.

This approach to assessment also has a number of methodological advantages, particularly when compared to assessment by mathematical expectation. First of all, the indicator $P(N \geq N_{ud})$ is much easier to use than mathematical expectation. For example, if we want to aim for an unacceptable (required) level of damage at around 1,000 warheads, while using mathematical expectation, we will have to "force" the composition of the SNF and the C^3 system in order to we reach this "point" in any case. That is because any difference between actual and assigned results would be considered "above" or "below" the requirement. Thus, there is no flexibility in the assessment – that point becomes carved in stone.

The indicator proposed here, however, completely changes the picture. The required damage level (1,000 warheads) can be established exactly, using the value of P (probability) as a variable. The range of variability is broad, from 0 to 1.0.

Second, it is possible to get a fuller and more detailed assessment of the enemy's strategy using the distribution function F'(N). Each type of strategy corresponds to a type of function (like fingerprints). Mathematical expectation, however, may obtain one and the same result with various strategies, i.e., that method is "not input sensitive."

Third, as noted before, the $P(N \geq N_{ud})$ indicator integrates the threat, acknowledging the possibility of both LOW and LUA. Such integration is not possible using mathematical expectation; simple averaging will not work here.

And finally, everything cannot forever be averaged. The answer to the question of whether we should challenge the status quo is definitely "yes." The stimuli are strong enough. Before thinking through the practical steps of this new method's implementation, the following chapter will look at some of the challenges ahead.

3.7 Implementation Problems

There are numerous problems on the way to implementing the discussed method. For the sake of the broader picture, three major problems come to mind:

First, how can we guarantee the acceptable accuracy of the risk estimate without hurting either side's national security? At first glance, the two parts of this problem seem to contradict each other, which is why we concentrate on this aspect. Obviously, if this contradiction is resolved, the method will be recognized as valid by the consumer; that is, the military and political leadership, parliament, the public.

Second, if the method comes to be seen as valid, a mechanism for implementing it should be created, initially for negotiations on strategic offensive weapons.

The third and final problem – the problem of choice – will always remain. That is, even if the method is accepted and the mechanism for its use has been created, what specific value should be applied as sufficient for reliable deterrence? This question is for both components – the value and the probability. And how will this deterrence indicator integrate with the general picture of strategic stability? What trends will appear as its value changes? What are the other aspects to consider here, besides the military and economic ones – moral, philosophical, political, etc.? It is certainly not possible now to provide decisive answers to all those questions within the framework of this third problem. We will try to deal just with some of them.

When analyzing the problems in detail, we will discover a whole series of derivative questions: overcoming natural difficulties arising from the classifying of initial data, that is, secrecy; the purely technical problem of representing initial data in probability formulas, including taking a human factor into account; the issue of trust towards the partner in the negotiations, and his behavior; as well as a whole group of other problems. We will try to address them below.

Though getting started on this path is difficult and seems to consist only of obstacles, let us not forget the advantages that, as we have become convinced, the suggested approach may bring. We have a motivation, and a very powerful one. Approaching the issue in a systematic way, we first tried to see the goal, then established its attractiveness, and now we look at ways of reaching it. In the very best sense, the goal here justifies the means. Let this idea support us while analyzing the most challenging and doubtful aspects, and let us say even in advance that, with strong motivation, they can all be overcome.

3.7.1 Accuracy of the Risk Estimate

The reliability of estimates under simulation, as we know, depends on both the pre-

cision of the model itself and on the precision of initial data. Let us establish at once that it is possible to create such a SIM, whose precision will satisfy the requirements for estimating degrees of risk. Remember that to estimate the degree of risk from the standpoint of deterrence, it is quite sufficient to go to one decimal: the probability of unacceptable damage at level 0.5 or 0.8 (not 0.73 or 0.76). In an extreme case, arriving at the second decimal presents no problem either.

The initial data are a different story. Whatever you enter into the system will determine the outcome. Errors in initial data may be much worse than the imprecision of the model itself. Therefore, we will pay all our further attention to the question of reliable initial data.

Remember that, in our case, the set of initial data includes, for each variant, a combination of nuclear weapon delivery systems, their C^3 systems, and the GIS, all of which, in a model, represent a graph of cohesion. The components of this combination are the graph's nodes, while the communications channels between them are the curves of the graph.

Let us now break the whole set of initial data into two groups.

The first group includes the data that determine the initial graph structure and its characteristics in peacetime. Assigning this type of data presents no great challenge for each specific variant. We take the required number of various types of delivery vehicles, establish their locations, then assign probability characteristics to all parts and curves between them for functioning in peacetime. The characteristics are determined by operational documentation and confirmed by experience; prospective systems use the system characteristics that are stated in the technical specifications.

The second group of initial data is the data that determine the probable performance characteristics of those same components during military action, taking into consideration an enemy assault with all available means. During a statistical simulation on the computer, each component and curve is randomly assigned, based on established probability, to a state of "yes" or "no." A summary result is then established from each simulation. These general principles of simulation have been discussed earlier, and we will not go over them here. Let us only emphasize that as a result of the enemy's attack, all probabilistic and temporal characteristics for all of the graph's elements will be worse than in peacetime. And the more optimal the enemy's strategy – that is, the distribution of his assault means between all the graph's components and curves – the better the result for the enemy and the worse for us. That is why, for each studied variant, we should try to establish the most rational strategies for the enemy.

How do we do that?

First, let us note that, for each separate type of component or curve (missile, submarine, command post, communications channel, etc.), the probability of its performance depends on the intensity of the enemy's assault. For example, it is known that in order to destroy a mobile missile launcher of n-type with a probability of 0.7, the enemy should use no fewer than 10 warheads of such and such power. If we need to increase

the probability, for example, up to 0.8, then we should increase the strength of attack up to 15 warheads. And so on (the numbers are relative). Each side has approved nomograms and schedules, which may be periodically reviewed and refined, but can be used in a concrete study as fixed initial data. This is true for all components and curves.

But all this applies to separately analyzed elements. "For the enemy," however, we have to distribute all resources for the entire graph. This is also not a new problem, and has been solved in many studies. We will pay attention only to two crucial aspects.

First of all, we have to determine which strategy is better for the enemy. Often it is thought that this criterion is the least number of our warheads launched. But we are already convinced that point estimates provide too little information. It is easy to demonstrate that we can arrive at the same minimal number N_{wh} under a whole series of very different offensive strategies. It would, therefore, seem more correct to use the entire curve of the distributive function F(N) (see 3.5.8) as the criterion. Here each strategy means a curve, so there is no ambiguity. Which curve is better? Let us leave this question to the consumer's taste. We will express some of our thoughts at the end of this chapter. For now, let us decide that we do have a fixed criterion.

Even that is not enough. To resolve the distribution problem, we have a criterion, an apparatus for each component, and data on the enemy's resources (approximated)! Now we have to go to the object of suppression – that is, our cohesion graph.

An attentive reader would ask: "But we do have our own cohesion graph; what's the problem?"

But the trick is that the graph in our possession is not sufficient. The enemy should have the above-mentioned data, too. Let us think – the solution for this distribution problem is a strictly bilateral process. It is as if we are thinking for the enemy, suggesting the strategies rational for him. How can he distribute his weapons rationally without any knowledge of the object to be suppressed? Thus, we have to consider the highest possible degree of knowledge on his part.

Here, it seems, we have arrived at our first really serious difficulty. The enemy knows his resources; we can reach agreement with him on the final criteria and nomograms for each component, but how do we take into consideration his knowledge of us? What does he know about the components, structure, and properties of our cohesion graph? Realistically, he needs to know about our SNF groupings, command and control system, and the GIS. But no side will completely reveal such data "off hand" because of concerns about its national security interests. Without those data, we will not be able to obtain results for the minimal deterrence levels. What are we to do?

We've come to one of the most important questions in this whole discussion – the question of availability of data, the question of secrecy. This is an obstacle on the way to our final goal, and as such, it should be resolved.

A few years ago, even posing this question made no sense. Today, there is a certain hope that it may be positively resolved, based on the experience each side has acquired in reducing nuclear weapons themselves.

Indeed, it has become possible to declassify the first part of our cohesion graph, such formerly super-secret areas as the number and types of nuclear warheads and delivery vehicles, as well as their deployment areas, and to establish mutual control over reducing them. Why shouldn't we be able to do the same for the second part of the graph, the command and control system and the GIS, without harming security interests of both sides?

Unfortunately, our thinking has been changing too slowly. Even now the opinion prevails that even if declassification of information about the weapons proper has become possible, command and control and information systems should never be.

This is certainly a mistake. In the first place, without resolving this question of access to command and control systems data, we cannot even talk about the problem of minimal deterrence. Analyzing only the weapons themselves, without including their command and control systems and the GIS, will not allow this problem to be resolved. Second, we ought at least to attempt to look at the command and control system from the perspective of which parts are "declassifiable" without harming the interests of national security. Perhaps our fears are somewhat exaggerated? Up to now, no one has even tried to analyze this. Let us try to do it now, at least on the most general level.

Let us break all the main data on the command and control system and the GIS into three groups.

The first group of data includes that information both sides know very well about each other, which make no sense to conceal. This will be easy to agree on. They include, for example, the locations and chief characteristics of the main stationary command posts and communication facilities; the presence of global command, control and communication systems; major cable routes; the parameters of standard communications technology; the nomenclature of the main components of the graph; and general principles of the command and control systems and GIS. After additional agreements, this list will complement our cohesion graph.

The second group consists of the data that should not be declassified under any circumstances. This group itself falls into two parts. One sub-group is the data that are of no importance for solving our problem. For example, there never is a need to let the potential opponent know the codes for blocking nuclear weapons (the so-called "State Number"), or the values for the encryption keys for communication channels. The other sub-group includes the data that have an influence over the graph's performance stability, but that should be declassified. They are, for example, the schedule of position changes by mobile nuclear weapons carriers and command posts, working radio frequencies, information transmission times, and others. Those are the very data that determine the probabilistic character of the graph components' performance, and are considered in the above mentioned standard initial nomograms and schedules. For example, the enemy knows that such and such type of mobile command post exists, he knows the approximate (or it may be declassified by our side) location, but does not know the frequency of position changes. An appropriate nomograms will answer the

question of what means are needed to destroy it with the required probability. Coordinating these nomograms with every component of the graph is a complicated business, requiring a lot of attention to detail and a lot of time, but in principle it is technically feasible. In any case, this is not a direct threat to national security.

Finally, the third group of data is those about which neither side is sure they know everything, and which also are relevant for estimating the cohesion graph. One example is data on the number of mobile elements of various types. Revealing the information would fill out the initial data and allow us to conduct our estimates. We will call such a completed set of initial data "fully revealed," endowing the word "fully" with a very specific meaning: we are fully protected against the enemy's penetration into our "state number," encryption keys, etc. This area of classified information remains intact. But let us note that this "full revelation" only touches upon the degree of stability in the command and control system's performance. Even so, the probabilistic character of much data has remained.

Revealing data from the third group would be highly desirable since it would allow us to start estimating results, but neither side is going to reveal it in a hurry. The reason is clear: no one knows what the final result would be. No one has "looked into it" yet. And there would be no way back from that point. In such a situation, the unknown would be frightening to anyone.

This is why there should be a logical intermediate step, an "insurance" stage for mutual theoretical studies using conditional initial data belonging to the third group, taken from a broad range. The goal of such studies is to obtain some guarantees that would allow us to become completely convinced as to the purposefulness of further work along those lines.

All previous arguments have brought us to the idea of such mutual research. It is absolutely necessary.

3.7.2 Towards Confidence Through Joint Research

What are the arguments in favor of joint research on the deterrence problem? First is the issue of confidence and guarantees.

No sensible person on Earth wants a nuclear war. Yet, "not wanting" is not enough; one would like to have confidence in stability. We have to get away from the vagueness of today's situation. Joint research with the use of the approach outlined above may help establish, first of all, a general theoretical picture, an "order" of deterrence indicators across the broad range of initial data. In other words, it would enable everyone to feel the scale of this new dimension – measuring fear. This in itself would provide some ground for confidence.

The fact that neither side would benefit from reducing the deterrence indicator to a level dangerous enough to destabilize the overall situation and increase the risk of war, would itself serve as a measure of guarantee.

The stability of the sufficiency concept may also serve as a guarantee, if it is con-

firmed by joint research (See 3.5.6). By that we understand that in peacetime, no side would be able to achieve such economic superiority over another that the degree of risk would make aggression acceptable.

Thus we can expect a "double guarantee" situation, in which neither side wants or can afford nuclear aggression. While everyone now accepts this intuitively, we will be able to prove this quantitatively.

There is reason to hope for confirmation of a stability area within the concept of sufficiency. This is betokened by the properties of the cohesion graph as a network. When the network reaches a certain size, the expense of expanding it becomes lower than the expense required to maintain its suppression at the previous level. To make this clear, let us review a simplified example.

Let us talk about a group of mobile command posts of the highest level. We are interested in the probability of at least one of them surviving. First variant – in the group there are four command posts. In order to eliminate one with a probability of 0.3, the enemy needs to allocate 10 warheads. The cost of one command post is one conditional unit. The cost of a strike by one warhead is 0.1 conditional unit. In this case, the probability of at least one command post surviving is $1\text{-}(1\text{-}0.3)^4 = 0.75$, and the relationship of the costs "group of command posts: attack" is 1:1. Second variant – we increase the number of command posts to six. With the same relationship between costs, the probability of one post surviving will increase to $1\text{-}(1\text{-}0.3)^6 = 0.87$. Therefore, the enemy will need more attack assets to maintain the same probability 0.75. For the attacker, the probability of survival of each command post should not be higher than 0.2. To achieve this result, the attacker needs to allocate not 10 but 15 warheads per command post, so that the relationship of costs will get worse for the aggressor, 1:1.5 instead of the former1:1.

Obviously, to reduce the probability of survival of at least one post to, for example, 0.5 or 0.3, the aggressor will have to allocate substantially more offensive weapons for this task. At that, the defending side is able to maintain this probability at higher levels with the help of lower, asymmetrical efforts.

This example illustrates only in principle a concept of sufficiency that is stable. If we consider not only a group of mobile command posts but instead the entire cohesion graph, everything will certainly become much more complicated. But the general trend, of cost ratio changing in favor of the defending side as the deterrence indicator decreases, should remain the same. To completely exclude (or achieve very high probability for excluding) an unacceptable retaliatory damage would probably be impossible. It is hardly possible to overestimate the significance of such a conclusion if it can be proved quantitatively. As noted earlier, this could solve a lot of problems.

It could demonstrate, for example, that no matter how great the potential aggressor's efforts are during peacetime, no matter how much he spends, and even with an optimal attack strategy, he will not be able to reduce the probability of receiving a retaliatory strike of at least 800 warheads to a value lower than 0.2 to 0.3. Is this a little or a lot?

Right now we are not making that estimate. The important point here is whether such an area of stability exists, while locating and confirming it would be the purpose of joint research. Let us remember that we will not have to completely reveal all initial data; all of this is possible using conditional initial data.

If we attempt to illustrate this idea it would look like this:

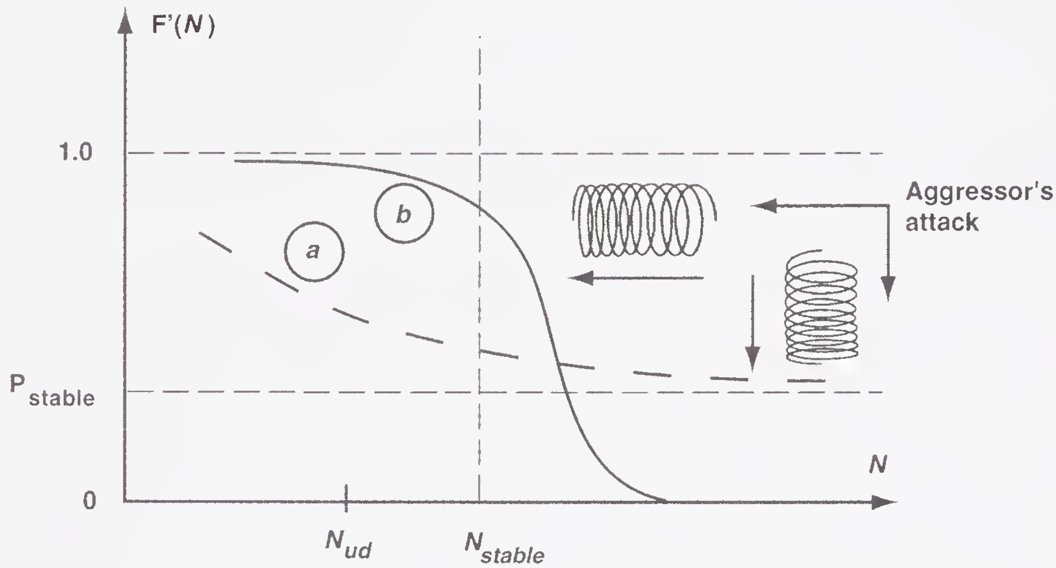


Fig. 27: The "Springs" principle with strengthening of opponent's attack.

Curves "a" and "b" are boundary curves corresponding with two extreme potential strategies for the enemy. Strategy "a" carries the risk of perishing – we will call it the adventurer's strategy; "b" brings a very costly (Pyrrhic) victory. Recall that with strategy "a" the enemy essentially "abandons" the N value and concentrates all his efforts on maximum possible reduction of the probability level P. To achieve that, when planning a nuclear strike he will have to allocate his main offensive assets against the cohesion graph's "broom handle" and the GIS. On the contrary, using strategy "b," he will have to "abandon" worrying about P, and concentrate most of his efforts and assets on the "sweeping" part of the broom, that is, the carriers of nuclear weapons themselves. In other words, he will try to reduce the N value to as low a level as possible.

The influence of the principle of stability is demonstrated in the fact that the lower are the values of P and N are, the harder it is for the enemy to reduce them further (the law of diminishing returns). This is like a spring working in two directions. In peacetime, the enemy tries to press the springs down and to the left, improving his means of attack. In reality, he tries to bring the curves of the distributive function F'(N) as close to zero as possible. The more he presses them down (that is, spends more resources), however, the less advantage he achieves, since the springs resist pressure. For the defender, though, the more the springs are pressed, the more favorable is the relationship between the costs of resisting the enemy and the enemy's expenditures. As noted earlier, at certain levels of P and N, this relationship becomes such that any further at-

tempts by the enemy to improve the expected result lose their meaning. These are the assumed stability levels. We will call them boundaries P_{st} and N_{st}. The whole purpose of joint research will consist, then, of establishing these boundaries as numerical values, so that later they may be compared with the P and N levels that are sufficient for deterrence. It is quite natural that the most favorable solution to this problem can be achieved through joint research.

It is worth emphasizing the independence of the results under various attack strategies. (See Fig. 28) For example, can the value of probability $P(N \geq 600)$ under strategy "b" be less than $P(N_{cud})$ under strategy "a"? This is true for our example: $P(N \geq 600) = 0.4$ and $P_{cud} = 0.5$, where "cud" is "clearly unacceptable damage." It seems this should not be so, yet it is correct, and easy to demonstrate with a simple example. Let us look at the whole complex of carriers, C^3 and GIS, as our already familiar "broom." (See Fig. 29).

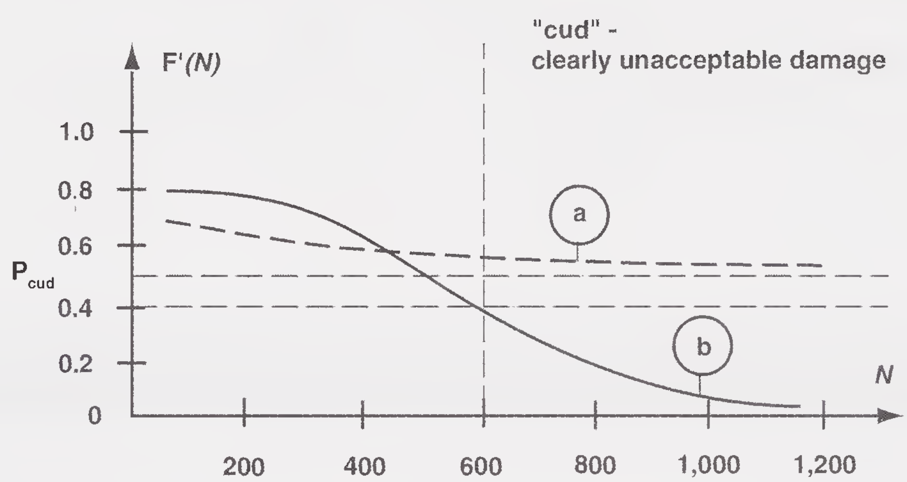


Fig. 28: Independence of results under "a" and "b" impact strategies.

When using the "a" strategy, the enemy allocates the major part of his assets for striking the "handle," thus bringing the probability of its performance down to 0.5. This means that out of 100 simulations, the "broom" remains undamaged in 50 cases. And what is the situation with the "sweeper" here? Since the enemy's attack was concentrated on the "handle," the "sweeper" is better off. In almost all computer simulations, the number of delivery vehicles and their warheads taking part in the attack is high and may be considered sufficient for unacceptable damage. That is, what we have in the "broom" altogether is: $P_{cud} = 0.5$.

If we change to the "b" strategy and concentrate the enemy's main attack on the "sweeper," we will achieve the effect seen in Fig. 31. The "handle" will perform in an even more reliable fashion: say, the probability of its performance will go up to 0.7. But in the "sweeper" the situation will worsen, so that in only about, for example, 60 of 100

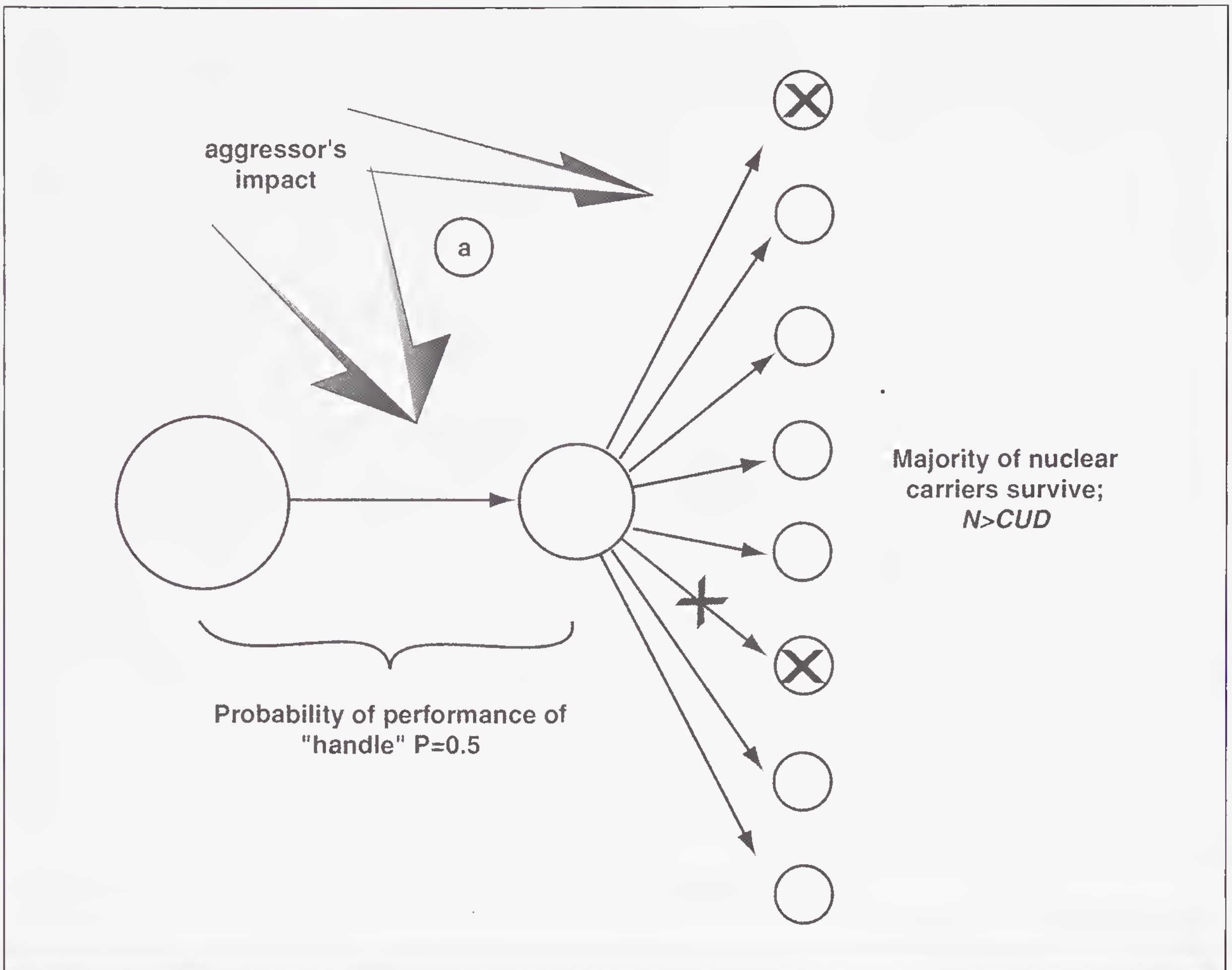


Fig. 29: "Broom's" condition under "a" impact strategy.

If we present the same picture through the density of the final result distribution, the picture will look like this:

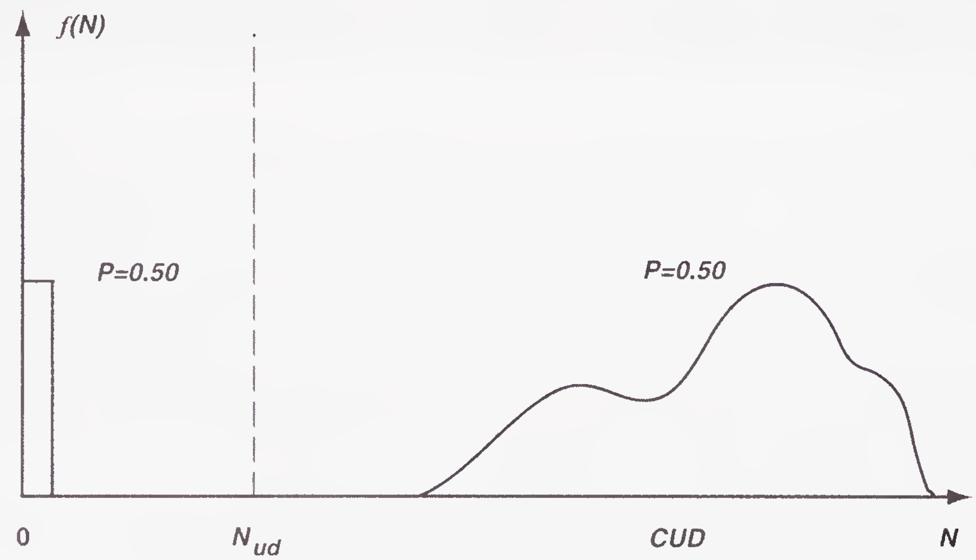


Fig. 30: The density of distribution (to Fig. 29).

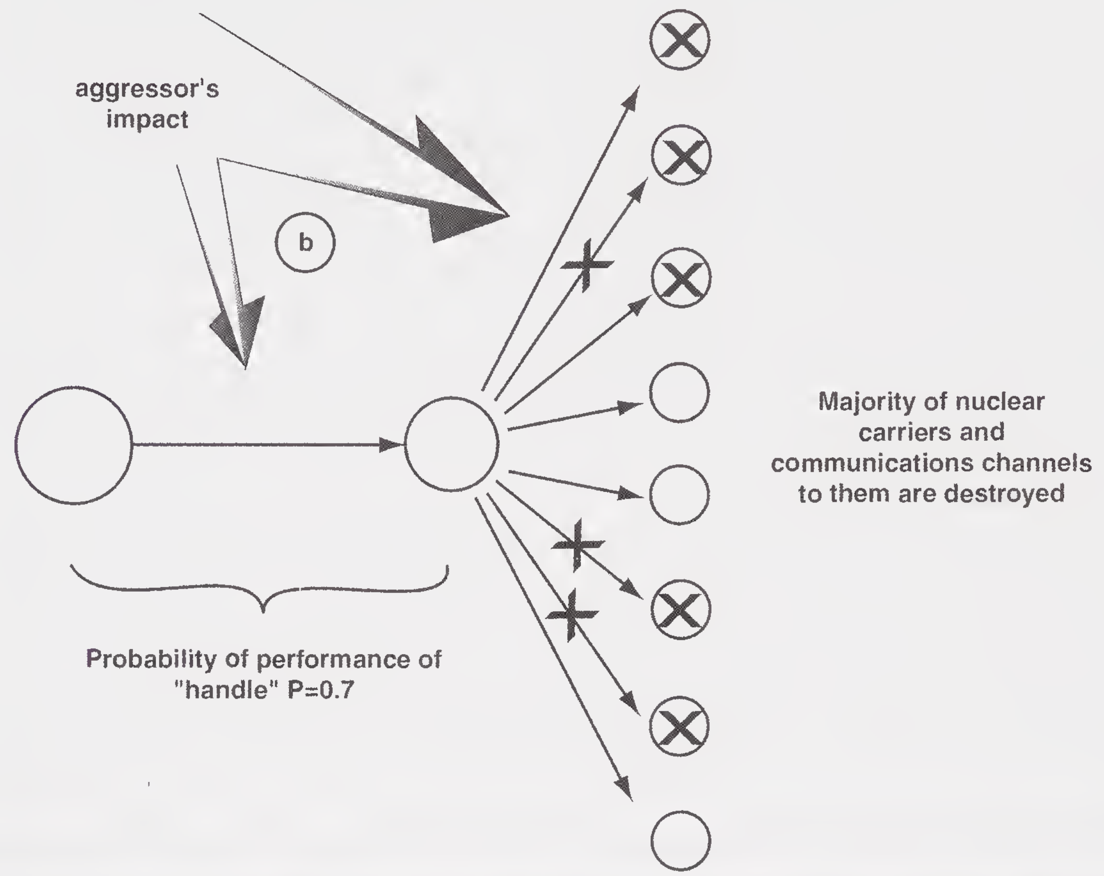


Fig. 31: "Broom's" condition under "b" impact strategy.

simulations will the number of warheads taking part in the strike be more than 600. We are interested in the general result for the whole "broom." Multiplying the probabilities of successive events, we will obtain:

$$\mathbf{P(N \geq 600) = 0.7 \times 0.6 = 0.42} \quad \text{(Fig. 31)}$$

So, even if the means of attack are redistributed from the same pool as strategies change, the final results may be considered to be independent of them. Results are determined by the structure and characteristics of the "handle" and the "sweeper." It is possible to have such a poor "sweeper" that, using the "b" strategy, not one computer simulation will result in the number of warheads being more than 600. Then, the general result is $P(N \geq 600) = 0$, even though the "handle" may be an ideal one in this situation. Each part of the "broom" plays its part and makes its own contribution.

The usefulness and possibility of joint research is influenced by the following simple logical considerations:

First of all, the very idea of mutual deterrence implies a mandatory exchange of in-

formation. Each side, after determining for itself a sufficient level of defensive potential, is obligated to demonstrate this to the opposite side. It is further required to prove that with such a potential, the probability of unacceptable damage for the aggressor would be of an appropriate value. Each side is most interested in seeing that the other side has this knowledge, or the deterrence factor simply will not work. Such a necessity is not felt very strongly right now because the current strategic nuclear forces are very large. Yet, when searching for minimally acceptable defensive levels, such mutual proofs will become crucial.

Second, this can be financially beneficial for both sides. The presence of fuller and more reliable initial data made available during joint research will allow the parties to come close to truly sufficient minimums and avoid unnecessary expenses. If the existence of the above described areas of stability is confirmed, both sides may avoid conducting expensive but pointless programs.

Third, there is no risk involved for either side. Each of the parties has the right to stop at the level that it deems sufficient for itself. And after conducting joint research, it will be able to obtain more solid support for its decision. How much initial data will be revealed depends, just as at the present time, on the specific situation.

Such joint research could have as its main goal fuller accounting of all major factors in the process of nuclear arms reductions, not only the initial levels of strategic forces such as composition, characteristics, deployment areas, etc., but also the possible final outcome of a nuclear exchange. It is, after all, not the potential itself, but the expected result of its use, that acts as a deterrent. And the latter, as we have seen, is most fully characterized by the probabilistic distribution value. Joint design and study of such distributions by both sides, and then using those studies to make recommendations to relevant agencies, is a viable way to speed up nuclear disarmament.

It seems that a logical first step in such work would be to agree upon the main methodological principles for evaluating the potential final outcome, and then selecting an appropriate model. With the help of these tools, still on a theoretical level and with the use of a broad range of conditional initial data, it would be helpful to elaborate on a few questions before going on to the practical steps:

- For how long, and down to what values, is the probability of inflicting unacceptable damage (or any assigned damage level) in retaliation on the aggressor sustained when reducing strategic weapon levels and deploying BMD systems?
- What are the boundaries of the existing areas of stability when, under any given spending levels, the defending side can, with relatively less effort than the aggressor, maintain a degree of risk unacceptable to the aggressor?
- What is the influence of realistically achievable and economically reasonable command and control systems on the character of probabilistic distribution of the final outcome, and what are the best ways to consider this factor during negotiations to reduce strategic nuclear forces?

Under what conditions is it acceptable not to consider any existing asymmetry in the potential of the opponents?

Once these and similar questions are answered, this methodological "tool" could be assigned official status for practical use during negotiations.

When discussing the practical implementation of this method, the problem of the so-called "human factor" arises. It is possible to establish probable characteristics for all technical aspects of the cohesion graph – command posts, information systems, communication channels, relay stations, etc. But, a human being also takes part in preparing the final result. Can we formalize, or "program," his activities? And doesn't this very serious consideration make the whole method doubtful?

The first impact of the human factor on the cohesion graph comes with the actions of the military political leadership upon receiving information on a nuclear attack from the Early Warning System. If we take all technical considerations out of the process, such as arranging the meeting, passing on the authorization, etc., the purely human process of thinking the information through, discussing the situation, and making the decision, will remain. It is no better than reading your fate in tea leaves to try to guess the probability of the leadership's performance, which depends on virtually thousands of moral, psychological and other conditions. What should we do?

A rather simple way to resolve this can be derived from the essence of the method, whose main feature is to consider the degree of risk for the potential aggressor. Let us look at the assumptions that the aggressor should make. He must plan for the worst. More specifically, he should plan for a situation in which the defending country's political leadership would perform ideally at the crucial moment, just as during the peacetime training, that is, would be able to respond within the "technical" window.

Mathematically speaking, the aggressor (and we are playing for him) has to assume that his "victim" will act with automatic effectiveness and speed (repeatedly confirmed during exercises) with probability of 1.0.

Agreeing on the value of this "technological window" should not present too much of a problem for either side. It cannot and should not be too much of a secret, but should be established during peacetime exercises. Recommendations on actions in a crisis by NCA were established some time ago on both sides of the ocean. Now, these leaderships have to have the final word. This will be their contribution toward the problem of quantitative measurement of the level of deterrence.

We also have to mention the crews at the command posts when discussing the purely human factor. These crews enter and issue the orders, either after the leadership has sanctioned a response or autonomously under the conditions described above. There is no need to repeat our study for the command posts after we have analyzed it in detail for the leadership. Everything applies, except for the fact that during peacetime, the military crews exercise on a regular basis.

The device we used above is one of the assumptions that are used in simulation, and

seems to be the most logical one. So far, at least, there has been no sensible alternative. If one is presented, it will not change the whole method but will only influence the initial data.

Now let us present an intermediate summary.

A priori, we have already overcome some methodological challenges. We have decided that our first priority is to establish theoretically a range of assumed values for the degree of risk, and to convince ourselves of the stability of the concept of sufficiency. This would be best done through joint research. If the safety margin of reliability is proved, the way will be open for the next practical steps. Then the two parties may cooperate on initial data that is lacking on a third group without any major risk to themselves. This process will be, it seems, of iterative character, with a gradual approach to the "truth." The path goes from redundant reliability towards a minimum reasonable reliability.

The transition from theoretical research to practical applications of the work will be a sophisticated business requiring patience, mutual understanding, and initiative on both sides. The results obtained will not be "points" but will be located within a certain range. At this stage, each side could justifiably rely on the following principle: any result obtained jointly, based on some accepted level of declassification for initial data, will be considered the "true" one. As the initial data become clearer and influence the precision of the final result, this will approach the "real" truth.

All this, however, will come at a later date. Today's agenda is to organize joint research between Russia and the United States, along with other partners, in this area. The purpose of this book is to establish the necessity of such research. All the following steps must be considered without losing sight of this final goal, or the motivation to achieve it. We also do not consider as closed the discussion of how to guarantee acceptable truthfulness in the final results, since this major question will be crucial for the two other problems in implementing our method: creating the mechanism for using it, and making choices.

3.7.3 The Mechanism for Applying the Method

Let us assume that a methodological apparatus for "measuring fear" has been developed through the efforts of both sides. A unified model has been created, and the existence of an area of deterrence indicator stability is proven theoretically. Now, the participants have started to discuss coordinating their initial data. This last step is, in reality, already a part of the negotiating process on strategic nuclear forces, since implementing it would get us closer to specific quantitative indicators for the command and control systems, GIS, and nuclear weapons delivery vehicles groups. Naturally, each side will check those results "at home" before coordinating any part of the initial data with its partner. Each side's behavior during negotiations will be based on those preparatory results.

Fig. 32 provides a schematic illustration of using the method during the negotiating:

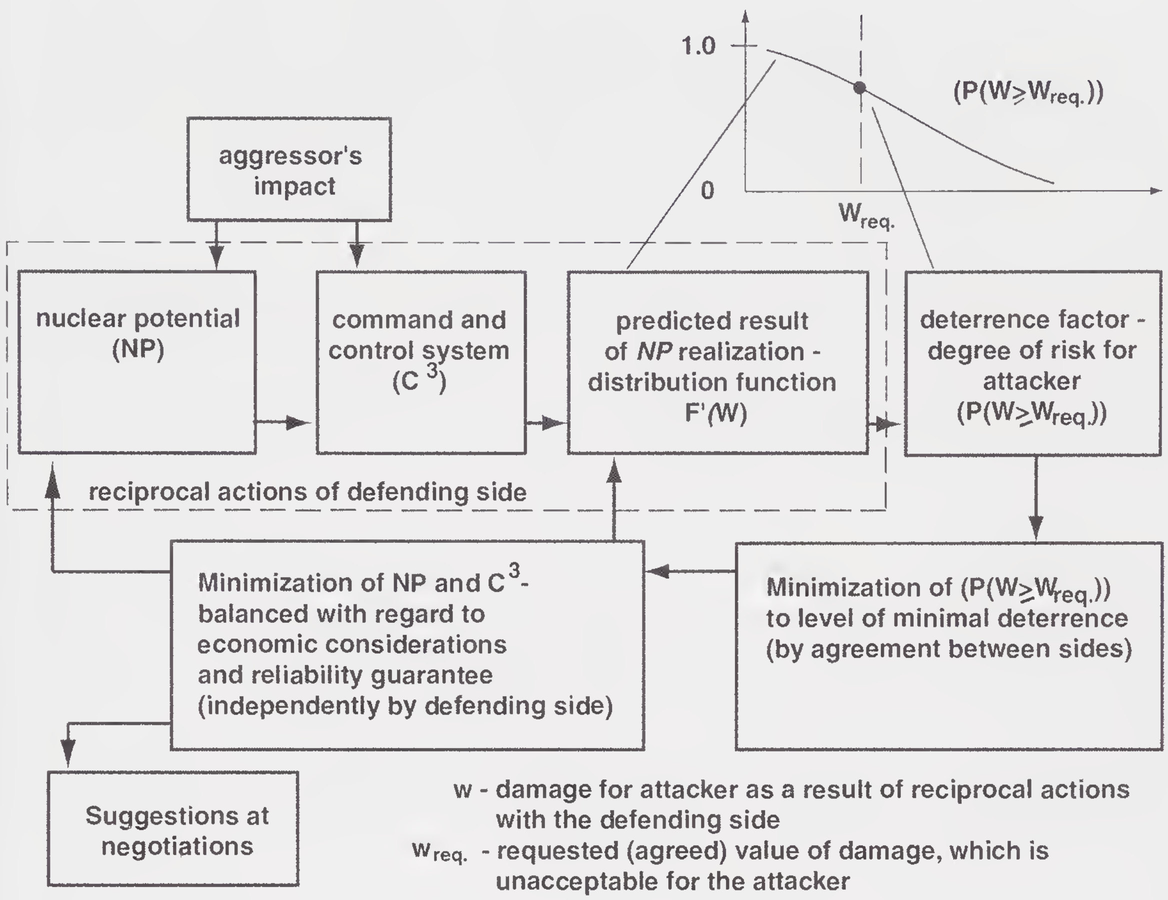


Fig. 32: The method for minimization of nuclear potential and C^3 factor.

Fig. 32 demonstrates that the final result of retaliatory actions by the defending side comes from the realization of its nuclear potential (NP) through (C^3), which guarantees the unblocking and use of nuclear weapons. Since both NP and C^3 are influenced by the aggressor's attacks, the result has a random character. Probability $P(W \geq W_{req.})$ is used as an outcome deterrence indicator in the illustration. Each side could use this indicator during negotiations to review questions of risk, deterrence, stability, etc. There is a possibility of flexibly manipulating its P and W components.

We may assume that it is possible to establish "threshold" values for the degree of risk according to the participants' mutual agreement. From the chart it becomes clear, however, that each side has the right to keep its "own" estimate of the degree of risk, and maintain a safety margin. This means that each partner may reduce his nuclear weapons, C^3 and the GIS independently, based on economic potential and other considerations. Only after many independent and joint estimates will each side present its balanced suggestions at the negotiations.

No matter how tempting this picture of joint projects is, its implementation may seem quite doubtful due to its highly unusual character: what guarantee does any side have that it will not make its own errors or be deceived? Everything depends on the behavior during negotiations. Let us try to analyze a few potential negotiating strategies.

The idea that the participants are interested in preventing a nuclear conflict as well as minimizing the cost of guaranteeing deterrence should be at the core of this analysis. The goal of analyzing potential behavior strategies at the negotiations is to try to minimize the level of distrust, both toward the other participant(s) and toward the potential results; in other words, to obtain certain guarantees.

Let us consider a possible Russian approach to the assumed strategies of the United States during such negotiations. This is just an example. It is logical to assume that the U.S. side is entitled to similar evaluation of the Russian strategy, taking into account their own peculiarities and interests. Can such an analysis, based on simple logical conclusions, help us find, in a preliminary fashion, some guarantees?

The following considerations should have priority:

The participants have worked out a joint methodological apparatus together, which gives them a model for estimating results they would like to predict. They have also agreed on maximum (critical) levels of indicator $P(W \geq W_{req})$ according to which they evaluate the results obtained in the course of research.

Russia evaluates the consequences of U.S. strategy according to three main criteria: does it change the degree of risk of nuclear war; does it reduce or create obstacles to the process of strategic nuclear force reduction, assuming this to be one of the main goals of world politics; and what extra expenditures will Russia incur, when purposeful outlays are separated from wasteful ones?

Our research indicates that those three factors are interrelated, so that, as a final result, improvements of SNF C^3 increase the value of the indicator $P(W \geq W_{req})$, while reduction of the SNF themselves decreases it. It is possible to regulate the indicator through balanced changes in the components and characteristics of SNF and SNF C^3.

When estimating possible U.S. strategies in the course of research, we assume the following attitudes of the United States toward the risk of unacceptable damage as a result of Russia's retaliation in response to a U.S. attack. For the majority of the public, the very possibility of unacceptable damage, regardless of its magnitude expressed quantitatively, is enough of a deterrent. For a minor segment (aggressive military/political circles, members of the military industrial complex, etc. – the so-called "hawks") just acknowledging such a possibility is not a sufficient deterrent. Additional quantitative estimates of the degree of risk $P(W \geq W_{req})$ will be necessary. This factor may play a deterring role only if it is officially and openly declared.

Let us demonstrate, considering all of the above, one possible Russian assessment of projected U.S. negotiating strategies.

Three lines of U.S. behavior might be used during joint research with Russia to obtain final calculations for the value of $P(W \geq W_{req})$. (See Table 4).

Strategy A: the "honorable" one, with the most reliable initial data possible. Two results are possible here: one, when the value of calculated indicator $P(W \geq W_{req})$ is high, i.e. higher than the mutually established critical level; and two, when it is lower than the critical level.

U.S. Strategy / Consequences of strategy	Strategy "A" ("honorable") results of calculations are:		Strategy "B" aims to increase the value $P(W \geq W_{req.})$	Strategy "C" goal is to decrease the value $P(W \geq W_{req.})$
	$P(W \geq W_{req}) > P_{crit.}$	$P(W \geq W_{req}) < P_{crit.}$		
Risk of nuclear war	small	high	high	small
Additional expenses of Russia for C^3 system	small	high	small	high
Continuation of START process (reducing nuclear arsenals of both sides)	accelerating	decelerating	accelerating (but it increases the risk of war)	decelerating
Attitude to the given U.S. strategy from U.S. side - Russian side -	most acceptable most acceptable	unacceptable unacceptable	for both: dangerous/ unacceptable	U.S.: partly acceptable Russia: unacceptable due to extra expenses
Conclusion and expedient measures	favorable situation: possible to consider next steps towards nuclear arms reduction.	necessary to agree on joint additional measures for increasing $P(W \geq W_{req.})$	U.S.: refuse "B" strategy; Russia: for insurance, to provide redundance: $+\Delta P$	U.S.: can use, maybe Russia: to try to increase P due to not only own additional expenses, but also with U.S. help.

Table 4: Evaluating the possible strategies of the United States side during joint research.

Strategy B: this one consciously aims at increasing the value of $P(W \geq W_{req})$ through artificial changes in some initial data, both American and Russian.

Strategy C: same as above, but with the conscious goal of lowering the value of $P(W \geq W_{req})$

We have to work under the assumption that it would be impossible to fully determine if the initial data was distorted by the United States. Therefore, while evaluating their strategies and our responses, we are forced to consider the possibility of such disinformation. Our ideas of how the United States evaluates its own strategies with regard to possible results should be of value to us here. Those assumptions are also presented in Table 4.

As a result of estimating possible U.S. strategies in the course of a joint research, we may draw the following preliminary conclusions:

Strategy A

a) If high values for $P(W \geq W_{req})$ are obtained in the course of the most "honorable" joint calculations possible, we may consider the main goal of effective nuclear deterrence achieved. In this case, we may consider the ways for further reductions of strategic nuclear forces.

b) If low values for the same indicators $P(W \geq W_{req})$ are obtained, the situation should be perceived as dangerous, mainly because the "hawks" will be strongly tempted to declare that aggression would not result in retaliation. Should such results be declared officially, the ensuing situation would have to be regarded as unacceptable for both sides, especially because the goal of further reducing strategic nuclear forces becomes more difficult. Under these conditions, both sides together will have to look for ways to increase the value of $P(W \geq W_{req})$ to a required level. There are several possible ways to do this: improve C^3 of Russia's SNF, or reduce the effectiveness of a U.S. conventional and nuclear attack against the Russian SNF command and control system, as well as against the delivery vehicles themselves. This could be done, for example, by redeploying SSBNs to the areas further removed from Russia, limiting theater and space armaments, etc. Naturally, further Russian steps for reducing strategic nuclear forces will have to take into account such considerations.

Strategy B

If strategy B is pursued by the United States, the calculated value of indicator $P(W \geq W_{req})$ is higher than the "true" one obtained as a result of "strategy A." Our (Russian) side may not have this information available.

This situation is also dangerous and unacceptable for both sides. The United States would still be tempted to commit aggression, because within the United States, those involved with the issue would know the true degree of risk, while society in general would not. On the surface, moreover, it would look as if it were possible to further reduce strategic nuclear forces. Such a measure, however, would actually increase the danger of war, since the value of the indicator $P(W \geq W_{req})$ would become even lower. Also, Russia would not feel a need to increase expenses for improving the C^3 SNF. For all these reasons, it is very improbable that the United States would use strategy B for joint research.

For Russia, such a U.S. strategy is also dangerous because of potential disinformation. Because establishing for a fact that information provided by the United States is or is not really disinformation is very difficult, we would have to take out an insurance policy, creating a safety margin in the value of indicator $P(W \geq W_{req})$. The ways to do that are described under strategy A.

Strategy C

Due to intentional distortions by the United States, the value of $P(W \geq W_{req})$ is lower than the "true" one. It is clear that in reality the risk of war is small. This is all the more so since, as in the case of strategy A (b), measures to increase the value of the main indicator would be taken. The implications of this situation are different for the United States and Russia.

It is not beneficial for Russia because we would have to incur additional (and in this case unnecessary) expenses for improving C^3 SNF. Or, due to the seeming weakness of

the C^3 SNF, we would have to slow the process of reducing nuclear strategic forces.

For the United States, strategy C is possible, if not ideal, under certain conditions. It is true that the risk of war would be small and might be further reduced. Russia would incur additional expenses. The only negative point (for the United States) would be slowing down the process of strategic nuclear force reductions. Nevertheless, this strategy leaves room for maneuver.

General Conclusion

When arranging for a joint research using the suggested approach, we may expect the Americans to be "honorable" in formulating their initial data, with a certain trend towards lowering the calculated values of indicator $P(W \geq W_{req})$. In this case, we should act with the maximum openness and accuracy of initial data, taking subsequent measures to create additional safety margin for the value of $P(W \geq W_{req})$. Those measures should be taken not only by us, but be met with countermeasures by the United States.

Thus the conclusions obtained through analysis may be viewed in the first approximation as some kind of a guarantee. While this example is just an illustration of the possible ways to choose, and is by no means final or complete, two advantages are obvious. First of all, the conclusion that it is impossible to totally exclude unacceptable damage for the aggressor may serve as a basis for guarantees for each side. If such a conclusion is confirmed by testing the initial data across broad, realistically achievable ranges, it may become a serious deterrence factor. Second, such a result, achieved during joint research by the participants, may in itself serve to increase mutual trust during the negotiations process and contribute to its success. Based on this, it would seem useful to consider an open exchange between the two sides of their own estimates of each other's possible strategies. After all, the goal of such activities – to avoid additional expenses while maintaining a reliable level of mutual deterrence – is very attractive.

3.7.4 The Problem of Choice: How Much is Needed for Deterrence?

Now, let us assume that the intermediate steps in our joint work have been completed. Areas of stability have been theoretically proven to exist. The quantitative boundaries of these areas – that is, values of P_{st} and N_{st} (st-stable) – have been elaborated. The next point on the agenda is an analysis of the cost-sufficiency of alternative variants of the totality of nuclear weapons delivery vehicles, command and control system, and GIS components, in order to select the most rational one that would guarantee reliable deterrence with minimal expenses. We will call this totality "SNF" for the sake of simplicity.

What considerations should we use for this choice?

First of all, we have to consider the possibility of the aggressor employing any type of strategy in his attack – from the "adventurer's strategy" (a) to the strategy of Pyrrhic victory (b). The aggressor can make this choice immediately before the attack by altering his choice of weapons to be used against the given targets. That is why our evalua-

tion of the result will have a dual character that logically follows from the dual nature of the deterrence indicator (P and N).

Second, we should take into consideration how a potential aggressor might evaluate the values of P_{st} and N_{st} obtained in the course of our calculations. Let us not forget that those are the maximum boundaries for "compressing the spring," that is at the highest possible peaks of arms race. If these same P_{st} and N_{st} are impressive enough to be a deterrent, then why "compress the spring" just a tiny bit more at the expense of huge financial outlays, especially since it won't do any good anyway? It would probably make sense not to plan for this senselessly intense competition, dreaming about supernatural and incredibly expensive weapons, but to follow the "natural" pace of development that is characteristic for the time. We should rather continue developing weapons, including means of attack against strategic nuclear weapons, C³ and GIS – but at an ordinary pace. This in turn means that during the subsequent series of bilateral estimates, the values of P and N, chosen as the reference points for the extreme strategies of attack, should be greater than the established values of P_{st} and N_{st}. The "springs" would be pressed down with less effort, corresponding with the real pace of weapons and countermeasures development.

We will call these practical reference points P_{pr} and N_{pr}, as seen in Fig. 33:

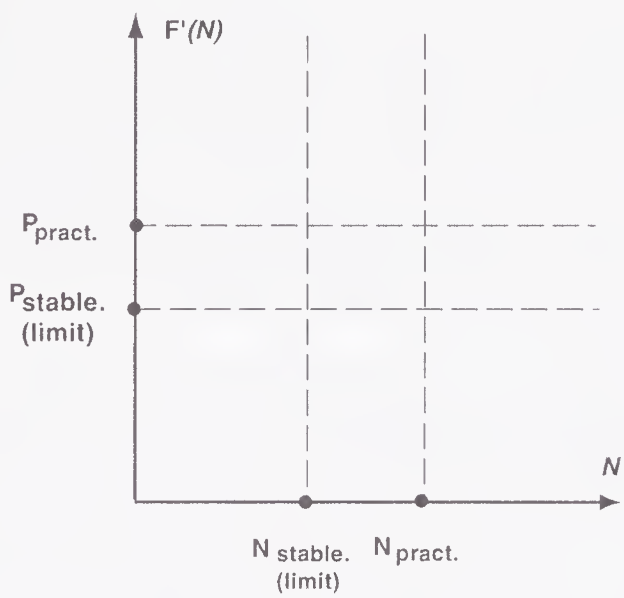


Fig. 33: Limit and practical levels of "springs" contraction.

For example, in an extreme case of arms race, the lower limit for the probability of unacceptable damage is 0.3, while in a "normal" pace of development it is 0.5. Accordingly, applying the Pyrrhic victory strategy in an "ideal" situation, we can calculate the minimum magnitude of retaliation at, say, 300 warheads, while realistically today and in the foreseeable future this minimum will be somewhere at the level of 600 warheads.

Or, considering the real situation, we have moved Area 3 of our picture up and to the right. We will do further work with this area.

What is our goal as a defending side? We need to have an SNF composition (including C^3 and the GIS) that would be able to provide for the curve of the distributive function F'(N) through Area 3 under any type of enemy attack strategy, from strategy "a" (adventurer's strategy) to strategy "b" (Pyrrhic victory).

In principle, we have to consider different variants of composition of SNF while modifying both maximum curves; that is, under enemy attack strategies from "a" to "b." Let us, however, note the following circumstance. Up to the present moment, as we have already mentioned several times in this chapter, no one has addressed the probability of damage (P), yet there is much debate about the magnitude of damage (W), and the concept of unacceptable damage remains quite vague. It will remain this way for a long time, and, quite possibly, over larger ranges.

Therefore, to simplify our further arguments, let us introduce the following device: we will analyze the variants of the SNF compositions while modifying only the "b" curve, leaving the "a" curve at a given fixed level. This device is justified because the "a" curve demonstrates the probability of enormous, known to be unacceptable damage (up to 1,200 or 2,000 warheads for example), and fluctuations within the 0.3 to 0.5 range are not very significant for this kind of probability. We have not yet learned to operate with such concepts. Let us remember also that the expenses for this curve go mostly for the GIS and the "broom's handle." So, we will assume that in all the variants of composition of SNF we will be reviewing, these expenses will remain constant and their size will be such that they will deter the enemy if he decides to use the "a" strategy.

The "b" curve is a very different story. Since the concept of unacceptable damage is so vague, it makes sense precisely here to review the alternative variants while taking into account the differences in costs for the other part of the cohesion graph – the nuclear delivery vehicles themselves and those elements of the command and control system that we have called "the broom." We will, naturally, consider general expenses when using the "sufficiency-cost" criteria while taking into account both curves "a" and "b."

One other consideration has to do with the time factor. Not only money and resources but also time are crucial to change any weapon development plans. For example, if the potential aggressor suddenly decided to change the expected picture, catch us unawares and go below the deterrence thresholds in order to later create the conditions for an attack, he could not succeed. Years are needed for developing and introducing into production and service new types of weapons, and to conceal them today is impossible. In this, case the potential victim would have time to take countermeasures. Such measures cost less than the enemy's (as we have demonstrated earlier), will compensate for the aggressor's efforts, and the threshold values of the deterrence indicator will remain at the same level. With a unified model and joint research, this fact will be easily demonstrable to the other side, and make it reconsider any abrupt changes in strategic stability.

Based on the above considerations, let us now consider as examples a series of results that could be obtained by analyzing alternative variants of the SNF composition for a specific period of time. All numbers are conditional.

Let us assume that there are four such variants altogether. First is the existing combination of weapon delivery vehicles, the GIS, and the command and control system. All other variants involve increasing certain components of this combination. We are not going into the details of what components are increased (according to their content and characteristics) right now. It is important, it should be done, and it should be done with expenses in mind. But this is "internal" work, while here we are limiting ourselves to an analysis of the general picture. Therefore, we will designate the expenses for SNF (costs – C) as ΔC.

The charts for the distributive function F'(N) for the given variants are shown in Fig. 34:

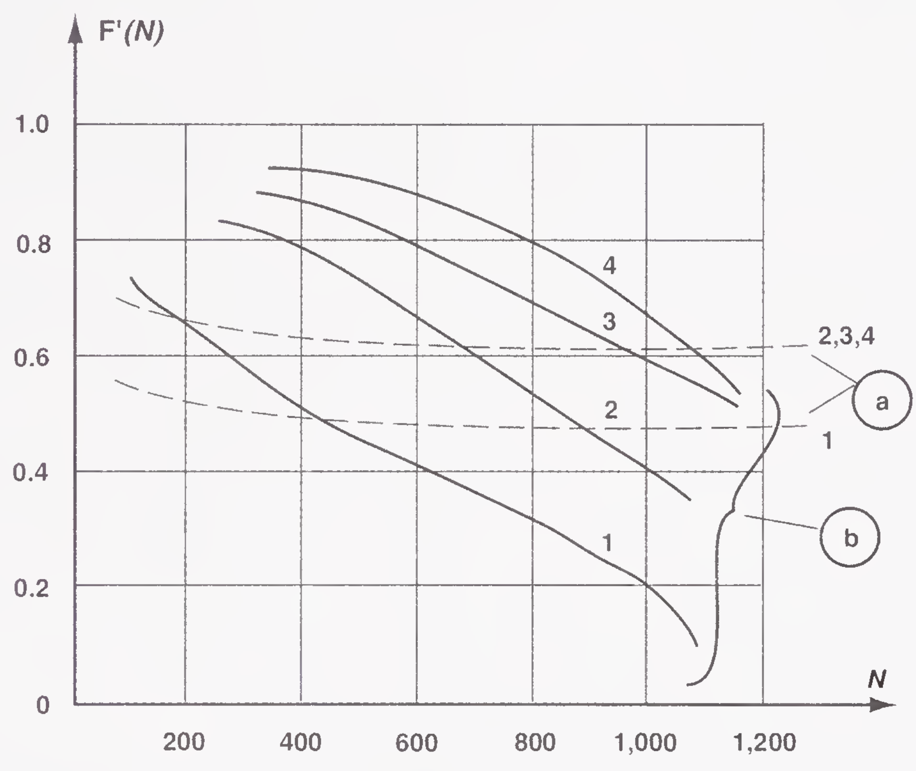


Fig. 34: Distribution function of final result for alternative variants.

These graphs provide the most detailed and complete characteristics of the given variants, and thus should serve as a basis for detailed analysis. When the variants are reviewed by a broad circle of users, however, it is more useful and convenient to use tables correlated with these graphs, such as Table 5.

"Clearly unacceptable damage" (CUD) – that which is maximally possible to achieve with the selected initial data.

How should a lay user view this table? The most important thing to consider when

SNF variant	Expenses ΔC (conditional units)	$P(N \geq N_{ud})$ under value of N_{ud}			
		under "b" impact			under "a" impact
		600*	800	1,000	clearly unacceptable damage
1	--	0.4	0.3	0.2	0.5*
2	2	0.7	0.55	0.4	0.6
3	3.5	0.8	0.7	0.6	0.6
4	6	0.9	0.8	0.7	0.6

Table 5: Evaluating SNF alternatives from the point of view of the deterrence effectiveness.

figuring this out is what damage value the aggressor perceives as unacceptable at a given time (ud). Let us assume that this has been established at the level of 500 warheads.

Besides, it is useful to see practical, maximum reference points N_{pr} and P_{pr} (in our table noted by *):

$$P_{pr} = 0.5 \text{ and } N_{pr} = 600$$

Now for the analysis of the table itself (Let us remember the theoretical boundaries of stability $P_{st} = 0.3$ and $N_{st} = 300$):

First the user looks at the potential result of the enemy's "adventurer's strategy" ("a"). The probability of retaliation whose value is "guaranteed" to bring clearly unacceptable damage to the aggressor is, in this first case, at the level of 0.5. It is located on the practical boundary of the area of stability, which means that as of now the aggressor cannot reduce it. But is this a lot or a little from the point of view of deterrence?

"Murphy's Law" is highly respected in the United States – here we call it the "Law of Bad Luck," meaning that if something bad can happen it will, and on the first and only attempt. In our case, "something bad" means the end of the world, and with a probability of 0.5. This is no Murphy's Law in reality; this is a 50/50 chance. Is it a deterrent? It seems to be. At least, nothing forbids the potential victim to raise this threshold up to 0.6 as in the table, or even higher if he has enough money. (Let us ask a provocative counter question: how much would YOU like for "full" confidence?)

Having finished with the "adventurer's strategy," the user will regard the other extreme: how tempted would the aggressor be to use the "Pyrrhic victory" strategy? How

"Pyrrhic" is this victory in reality? Would the damage be that unacceptable even if retaliation is highly probable?

Let us look at the table. If we consider that 600 warheads is close to the lower boundary of unacceptable damage (we established in the beginning that $N_{ud} = 500$), then variant 1 seems weak since $P(N \geq 600) = 0.4$. We can say that our "sweeper" is not complete. Even if the enemy should declare that these conditions are enough of a deterrent for him, we nevertheless have the right to chose variants 2 or 3.

If the damage is considered "unacceptable" at the level of 800, not 500 warheads, which variant should we choose? Variants 3 or 4 seem most likely. If $N_{ud} = 1{,}000$ warheads, we may have to review potentially more expensive variants, etc., etc.

What is left now is to integrate the result and present as concisely and graphically as possible. What have we got? If our initial conditions state the lower boundary of unacceptable damage as 500 warheads, we recommend:

Choose variant 2. It is least expensive and guarantees $P(N \geq 600) = 0.6$-0.7. If we select the more expensive variant 3, this indicator will be higher: $P(N \geq 600) = 0.6$-0.8.

Dear users, make your choice! "Our products are guaranteed."

Let us note here that the range of presented values of the probability we are seeking is not just a simple "fork": 0.6 is P_{cud} and 0.8 is $P(N \geq 600)$. Therefore, for general use, we may suggest the following formula for the deterrence indicator:

$$\mathbf{P\ (\infty \rightarrow 600) = 0.6 \rightarrow 0.8.}$$

The infinity sign here indicates the level of completely unacceptable damage.

Perhaps someone will be able to think of a more interesting and elegant formula, but the important point is that everyone should be able to understand it.

All figures presented here are, of course, conditional, by way of example. But even if they were obtained as a result of joint research, our recommendations still should not be taken up because we cannot – have no right to – recommend a specific level of deterrence. This is a task for everyone, and one that should be solved democratically. What is presented here is a tool, a method for this task. Recommendations presented in this chapter should be perceived as suggesting an order of choices, not conclusions according to specific values.

Chapter 4

C^3 in Russia and the United States: A Comparative Analysis

4.1 Russian C^3: History of Establishment and Development

4.1.1 The Beginning Stage (1959-1964)

The formation of the SNF C^3 began and has improved together with the formation and development of the forces themselves. With the appearance of the first nuclear weapons delivery vehicles (long-range bombers, short-range and medium-range ballistic missiles), they were taken under the strict and centralized control of the supreme level of the Soviet military-political leadership. The main functions of nuclear command and control – blocking unauthorized use, development of operational use plans and perfecting procedures for direct management of nuclear strikes – were the exclusive prerogatives of the General Staff.

The lower level command and control organs of the Ground Forces, Air Force and the Navy had the tasks of routine command and control over the weapons' condition and maintenance.

Initially, engineering brigades for nuclear ballistic missiles were included in the composition of the Supreme High Command's reserves. The 1959 appearance of a new military service – the SRF – was a huge step in regulating command and control of the rapidly developing nuclear weapons, and was used to create better conditions to develop the doctrinal and technical foundations for using this fundamentally new means – as they thought then – of warfare.

Today, everyone officially recognizes that nuclear armaments must not be used, and that they may be regarded only as a peculiar means of deterrence. However, this perspective assumes the necessity of a more-or-less logical theory of their use.

The nuclear doctrine of the early 1950s freely accepted the possibility of nuclear war. On Sept. 14, 1954, in the Soviet Union's southern Urals village of Totskoe, a 20-kiloton bomb exploded at an altitude of 350 meters. Thirty-seven minutes after the explosion, "attack" troops wearing protective clothing passed through the explosion's epicenter. The fact that nothing immediately happened to them gave the Soviet establishment a basis for developing a broad campaign to disperse the fears associated with nuclear weapons. For some time this succeeded. In spite of the widely known long-term consequences associated with Hiroshima and Nagasaki, many in the Soviet Union, especially the military, began to think that "there was nothing to fear in it." Unfortunately, the inertia of this impulse proved quite strong and, for many years, defined the character of military-ideological goals.

During a review of the Totskoe exercises, Nikolai Bulganin, then minister of defense, drew attention to the necessity of developing troop operations in a nuclear contaminated zone. Nikita Khrushchev further used these "results" in the political struggle with Malenkov, accusing the latter of ignoring real experimental data which, according to the general secretary of the Communist party, confirmed the admissibility of nuclear war.

Officially, this position was embodied in the so-called "Sokolovsky's strategy." Its appearance is connected with the publication of *Military Strategy*, edited by Marshal V. D. Sokolovsky. In the book, basic elements of conducting a nuclear war were formulated, and they defined the main trend in the subsequent development of Soviet military theory, including the operational and technical aspects of nuclear command and control.

The main question then was the ability to maintain command and control of troops under nuclear warfare conditions. Official assurances that this was the case in the Soviet military were pure bluff, and were actually refuted in the General Staff and the scientific research institutes' classified materials. Everyone understood that at that time there was no technical basis for command and control of nuclear war.

At first, in the process of establishing nuclear forces, command and control was accomplished using the existing communications networks of the military districts, other services and civilian administrations. The overall technical level of military and civilian communications was quite low. Here, antiquated types of telephone and telegraph equipment were in use, as well as radio stations many of which were pre-World War II design. Secure communications were practically nonexistent, and therefore the sole means for transmitting important information was ciphered communications, with all of its complications and low efficiency. Special difficulties arose in organizing command and control of the new SRF sites due to their isolated location.

Additionally, from the first day of the nuclear forces' life, demands for reliability, efficiency and secrecy in their command and control became rigid. All existing methods had to be investigated in order to mitigate the sharp contradiction between big wishes and very limited capabilities. For that, the scanty resources of the local civil networks of the Ministry of Communications were exploited to their limit in the interests of the new users. The best mainline channels of cable communications with Moscow were relinquished to SRF on an around-the-clock lease.

But even this was not enough, especially for the proposed period of military operations. Therefore, based on a special government decree an operational system was introduced, allowing nuclear forces in extraordinary circumstances a significant additional number of the Ministry of Communications' cable and radio channels. All of these channels were pre-assigned to specific sites, and their transfer to the SRF units was regularly practiced during exercises and training. Besides, urgent subscriber connection by any of the other civilian channels, in case all available military channels went out of order, was often used. In this case, by transmitting down the line the set password *Vozdukh*! (Air attack!) or *Samolet*! (Aircraft!), the existing regional and district communications centers, within one to two minutes, enabled communication between

nuclear sites separated from each other by thousands of kilometers.

The absence of industrially-manufactured means of command and control, which would correspond to the high requirements, forced the creation of temporary, home-made substitutes. During these formative years, innovative activities were prevalent within SRF, naval and airborne SNF units. Different types of command post panels and displays, crew training simulators and secure communications equipment with set crypto-stability level were created by specialists within these units. Of course, these automated systems did not play a decisive role in improving nuclear command and control. Still, independent inventions were distinguished by originality and, in several ways, such initiatives by young officers helped to speed the creation and introduction of a new standard of work.

As a whole, the old technological base created large problems in managing the fledgling nuclear forces. The Ministry of Communications' cable network, on which the command and control system operated, worked intermittently, often having long breaks in communications with sites. The use of radio communications was severely limited because of secrecy considerations. Satellite communications did not exist in practice. Command and control deficiencies became especially noticeable in command and staff training exercises, where it was clear that they were slowing down further refinement of operational command methods. The transmission of orders and receiving of reports were carried out, as a rule, by telephone, with a large number of corrections and clarifications. The documentation of generalized data was carried on manually, with officers from the staff assigned to follow the operations of each corps and division, and specially-selected officers who took note of data on missile launches, etc. Frequently, the purpose of entire exercises was to try to clarify how many missiles accomplished their mission, and how many were destroyed by the "enemy." It became clear that the fundamentally new weaponry required a fundamentally different command and control system.

4.1.2 The Transition to the Automation of Command and Control (1965-1970)

The growing sophistication of nuclear missile weaponry and methods of its use brought to light the question of a transition to automated command and control. The experience of the first several years of combat duty allowed a sufficiently clear formulation of the basic requirements for a future automated system of command and control (*avtomatizirovannaja systema upravleniya*). It had to support, first of all, highly reliable, fast and secure transmissions of orders for missile launch.

Of the three mentioned requirements, speed became the main one, in that practically all scenarios "gamed" during exercises envisaged the exchange of massive nuclear strikes, after which the Soviet system was, justly, considered to be completely destroyed (however, in the opinion of Soviet and American experts, the same outcome applied to the American system). Although the open press remained silent about the given circumstances, the people inside the military-industrial complex had to make a choice: either to create a command and control system so survivable that it would be undam-

aged in nuclear war, or to make one so fast that it would succeed in launching all missiles in the intervening time from the warning signal of an attack to the arrival of the enemy's first nuclear warheads.

The emphasis was placed on the so-called response-encounter strike (OVU – *otvetno-vstrechnyy udar*) – the American terminology, launch on warning (LOW). In reality, such a concept did not in the least disturb simultaneously gamed follow-on operations after exchange of strikes, i.e., to re-establish the command and control system, to re-target the remaining missiles and to conduct repeat launches for the "final" victory. This was the concept of response strike (OU – *otvetnyy udar*), or launch under attack (LUA).

War gaming on military maps had to be supported by actual development of appropriate command and control means by industry. It was decided to finance both concepts, although, notably, less financing was allotted for the second one. At the early 1970s, successes in space technology predetermined the selection of LOW with the strengthening of the ground missile strike EWS by satellites. The SNF's command and control system now had "improved eyesight."

Besides the struggle to gain seconds, necessitated by essence of LOW, high reliability would be required from the future automated command and control system, both in peacetime and in limited conventional warfare. This requirement was not easy to accomplish, if one keeps in mind the deficiencies of the existing communications network on which the automated system had to rely. And, of course, besides the major function of bringing the launch orders, the new system had to support day-to-day management of troops and remote monitoring of the missiles' technical condition.

By the beginning of the 1960s, there were two main directions for developing such a command and control system. The first was characterized by the idea of using special integrated circuits in the automated system. This, according to the designers' intent, was supposed to provide relatively flexible logic for using nuclear weapons, i.e., to change, if necessary, the automated system's working algorithm by re-programming. This direction was promoted by the Moscow Research Institute of Automatic Equipment, led by Vladimir Semenikhin (subsequently, member of the Academy of Sciences).

The other proposed direction for an automated system used elements with rigidly-fixed ("hard-wired") logic, produced on ferrite-cores (*Ferrit-ferritovye yacheyki*). Taras Sokolov is rightfully regarded as the father of this direction. At the end of the 1950s, while working as an instructor at the Leningrad Polytechnic Institute – LPI, Sokolov had already worked out and successfully put into practice the ferrite-cores idea. In 1961 he established a research design bureau attached to the LPI (presently the Scientific Production Corporation – the Impuls Corp.) and invited his most capable students to come there. These were, basically, young graduates of LPI who challenged the recognized authorities from Moscow. By 1964, the LPI Design Bureau completed the development of a highly reliable ferrite logic board sealed in a special compound. Based on it, the first experimental pieces of SRF command and control equipment were built by the end of 1965.[115]

In the history of the Soviet military-industrial complex, there have not been many instances of real competition for a huge order. More often than not, matters were decided on a monopoly basis according to an edict from above. The story just discussed could be considered an exception, and the subsequent course of events confirmed the undoubted usefulness of such a form of selection.

Parallel research and development ended with competitive prototype testing, conducted in the first half of 1966 in Moscow and Leningrad. The struggle was for obtaining the SRF automated command and control system order, since the country's fundamental efforts in those years were concentrated on supporting rapid establishment of this service. Officers of the Ministry of Defense research institutes and from the troops (mainly from the SRF) were assigned to the Moscow and Leningrad operational trials. I was among them.

The competitive trials, which lasted for several months, were capped by Sokolov's victory.[116] It turned out that equipment based on the rigid ferrite-cores-logic notably exceeded in reliability the analogous devices, based on still imperfect integrated circuits. At the same time, a relatively small set of commands and reports, "hard-wired" into the automated system developed by the LPI special design bureau, was fully sufficient for SRF command and control of that period. For the sake of objectivity, we will note that later the Leningrad group also made the transition, gradually, to more flexible computer logic, but with greater reliability.

In spite of the definite resistance of several highly placed individuals, in particular the then minister of defense, Marshal Dmitry Ustinov, the creation of an SRF automated system was entrusted to Sokolov. In view of the limited resources of the LPI Design Bureau, and based on several other factors, coordination of system development for Naval and Air SNF was entrusted to Semenikhin. He was designated as the developer of the authorization system for nuclear forces use, and afterward as the general designer of the command and control system for the entire Armed Forces. This division of influence between developers of the automated system has been maintained, in principle, until this very moment. Today, however, there are definite tendencies toward combining future work under a unified leadership. We will address this below.[117]

4.1.3 Main Development Stages of the Soviet SNF Automated Command and Control System

(A) *The Highest Level of Command and Control*

The highest level of the Soviet nuclear command and control was established at the end of the 1950s with the creation of the nuclear forces themselves. It included the Defense Council, headed by the supreme commander in chief (*Verkhovnyy Glavnokomanduyushchiy*); in the Soviet Union, this was the general secretary of the Communist Party of the Soviet Union and the General Staff with its corresponding directorates and system of command posts. In practice, this structure has been invariably maintained until the present time, except that the supreme commander in chief is now the Russian president.

The functions of the highest level of nuclear command and control, the most important of which is making decisions together with the political leadership on use of nuclear weapons, have not changed much since then. At the same time, the technical foundation of command and control – the system of command posts and corresponding means of automated command and control – have evolved quite substantially.

Until the early 1970s, work in the highest levels of SNF command and control had mostly not been automated. Information from the troops was collected by telephone and telegraph. The necessary calculations and generalized data input to the display in the General Staff's Central Command Post were performed by hand. The same can be said about the work of the NCA. During a period of threat, they were supposed to gather in one of the heavily protected underground bunkers, which could, in principle, survive nuclear strikes, but which were not equipped with effective means of automated command and control.

The General Staff's Central Command Post transmitted nuclear employment orders to the troops primarily via the Monolit system. The Monolit simultaneously transmitted via cable and radio coded signals to be decoded at reception points by opening special packages, which were kept under strict control in the safes of the troops' command posts. These packets had been prepared beforehand in the General Staff, then circulated to the troops, and were periodically updated.

The Monolit system had existed even before the establishment of the Soviet nuclear forces. One must give credit to the military signals specialists who ensured for many years that Monolit improved troops' command and control. Many crews were virtuosos when it came to receiving Monolit's radio transmissions under powerful jamming by the "enemy." Individuals, designated Champions of the U.S.S.R. and Europe in ham radio operation, frequently served on duty at the most crucial elements of the command posts.

However, the new weapons' stringent requirements for command and control pinpointed the main shortcomings of traditional types of communications, including the Monolit system. After the order was received through that system, the missile launch operations could be carried out (or not) only by the crews at the lowest levels of the nuclear forces. Remote launches or their urgent cancellation, originating from Moscow, were impossible. The old system's speed was also no longer satisfactory.

Members of inspection teams, which frequently visited the troops during exercises, time and again witnessed how outdated Monolit had become even from the psychological point of view. In a decisive moment, a duty officer of the combat crew might fail, sometimes for several minutes, to cut open the packets with scissors because his hands were shaking so badly. One does not know what frightened the officers more – an imaginary nuclear war or the real inspector from Moscow, calmly observing this unique procedure. In any case, minutes – crucial for evaluating the combat readiness of a regiment or a division – were wasted.

The problem of using scissors was recognized as so serious that troop inventors were entrusted to find the solution. The packet was constructed with a pull-string, on which

an operator could tug to immediately open the packet. In operational documents, the combat readiness was thus increased by 18 seconds, although in reality it was, most likely, greater.

The situation changed in many respects during the 1970s. Under the guidance and efforts of the cooperative headed by Semenikhin, a series of automation techniques was developed and introduced at the highest level of command and control, improving the quality of nuclear command and control. Important roles in their creation were played by the designers Mikhail Loginov, Victor Konashev, Igor Mizin, Yuri Leshchenko, and the military customers: Marshal of Communications Troops Andrei Belov, and Gens. Vladimir Druzhinin, Eugeny Evstigneev, Anatoli Zimenkov, Victor Mikhaylenko, Vladimir Shutov, Konstantin Trofimov and Yuri Ryabinin. Three of the latter were tragically killed in 1987 in an aircraft disaster in Hungary, during a mission concerning equipping the troops of Warsaw Pact countries with automated command and control systems.

The basic automation systems for command and control at the highest level included the authorizing system *Kazbek*, the notification system *Krokus*, and the system for combat command and control KSBU (*kommandnaya sistema boevogo upravleniya*). Beside that, at the Central Command Post of the General Staff, the *Signal* automated command and control system was installed. This system was developed by the Leningrad group of Sokolov. With the help of KSBU, the General Staff exercised command and control of the airborne and sea-based SNF, and likewise of the Armed Forces as a whole. Through *Signal*, SRF command and control was accomplished. These systems are described in more detail in the next section.

A look back at the history of creation and development of KSBU will show the following. In contrast to the *Kazbek* and *Krokus*, developed and introduced into operation in a rather short period of time between 1978 and 1983, the development and introduction into operation of this large, multi-level system dragged out for many years. Its development had begun in the early 1960s, but it was officially accepted as a complete operational system during state tests under the command of the chief of General Staff, Marshal Sergei Akhromeev, and put on combat watch only in 1985. Until then, separate elements of the system were in experimental use by the military.

Such a long gestation period was due, for the most part, to a not altogether successful approach by the customer. Instead of introducing one KSBU element at a time and relying on intermediate versions of the system, the military constantly advanced new requirements which resulted in significant additional work on experimental sections, after which new requirements were advanced, etc. This vicious circle was broken only when Akhromeev took charge of the program. Akhromeev paid considerable attention to the KSBU and enjoyed a good relationship with its general designer, Semenikhin, who had considerable influence upon the Soviet high command. The prestige of Semenikhin's firm weakened only in the last years of his life (he died in 1990), mostly because of reduced interest in command and control and because of the general problems in the Soviet Union.

During the last decade, a high-level command and control system has been developed within the framework of the Armed Forces global command and control project, named *Tsentr* (Center).[118] The highest level in that system is called *Vershina* (Summit). The projects are intended to enhance reliability and speed for preparing authorization, to automate collection of information and analysis of the operational-strategic environment, and to introduce some new means of C³. However, the political turbulence of the 1990s has somewhat slowed down the implementation of these projects.

(B) The SRF Command and Control System

The SRF moved toward automation of command and control independently. Despite Semenikhin's closeness to the powers that be, and his sharp competition with the Leningrad group, all the command and control issues for the main service of the Soviet Armed Forces were decided by SRF officers and the LPI Design Bureau. The General Staff was involved in the details only when it came to protection against unauthorized use, plans of combat employment and integration of the SRF automated system with the highest level of command and control.

The history of how the creative collaboration between SRF specialists and civilian scientists grew and developed is interesting in itself. It shows that even under the bureaucracy it was possible – in a relatively short time – to create from scratch the basis of a theory of nuclear command and control, to develop and manufacture the necessary technical means, and to equip the troops with them.

It is a striking historical fact that the basic concepts of nuclear command and control, such as protection from unauthorized actions, remote monitoring of weaponry, retargeting, the degree of automation of launching processes, efficiency, reliability, etc., originated and obtained real maturity in the minds of the General Staff and SRF Research Institute specialists, but also, to a similar degree, in the purely civilian team of the LPI Design Bureau. More than that, not bound by the narrow confines of military tradition, Sokolov and his young colleagues, Vladimir Petukhov, Boris Mikhailov, Leonid Vasil'ev, Anatoliy Greshnevikov, Vitaliy Mel'nik and others, provided many new ideas precisely for the command and control doctrine. These and other designers of SRF C³ systems are the subject of published memoirs by their SRF colleagues and veterans.[119] Their ideas were immediately discussed with the military in Leningrad, in Moscow, at the SRF Research Institute in the Moscow suburb of Bolshevo, and then implemented at the design bureaus and factories of the Leningrad research, development and production network. Nobody, in essence, hindered the Leningrad team's work, money was regularly disbursed from above, and the appropriate results appeared soon enough.

Already in 1967-1968, the first serially produced levels of the *Signal* automated system had begun to enter service with SRF formations. Equipping the troops went from the bottom up. First, they created the equipment for the command posts of medium-range missile battalions and regiments, and of ICBM regiments (levels 6 and 5). At the same time, in the Design Bureau all the other levels of the *Signal* system were devel-

oped – for the missile division (level 4), army (level 3), and the SRF main staff (levels 1 and 2). These types of equipment were given to the troops later, with delays of several years each. For the training of troop officers, courses were set up in Leningrad and Moscow, and at the strategic missile sites.

The *Signal* automated system, belonging to the first stage of automation (the late-1960s through the mid-1970s), allowed transmission of 13 fixed commands concerning the establishment of watch or combat work modes for the system, the transition of troops to various readiness levels, the number of the combat plan to use, and the order concerning the start and cancellation of a missile launch. There was a provision for gathering up to 20 confirmations and reports in response to previously prepared questions concerning the state of missile and troop readiness, delays, and mission accomplishment.

During that stage, missile launch installations themselves were equipped with another device, not included in the *Signal* automated system. This was the so-called remote command and control and monitoring system (SDUK – *sistema distantsionnogo upravleniya i kontrolya*).[120] Designers who worked on launch positions developed its several variants. The SDUK, on one side, was joined to the rocket, and from the other – by an underground cable – to the automated command and control system at the lowest level of command post. And, although a variant electrically joining the automated system and the SDUK directly was envisaged, the primary mode of *Signal* system use was assumed to be manual, when the crew carried out launch operations at the divisional or regimental command posts after receiving the order from above. Therefore, the first-stage automated system was called a system of troop command and control, but not yet of weaponry.

Equipment of the first generation was quite large and required considerable power, especially at the division level. Its external deficiencies, combined with limited operational capabilities, evoked criticism from competing designers and did not allow the technical solutions to be used in the interests of the entire Armed Forces. However, in the SRF itself, the benefit of the first modest step was immediately felt. Actual operational experience not only revealed technical deficiencies, but gave a powerful surge to questions of operational nuclear command and control. Not a single SRF exercise was now performed without the use of the automated system. Duty crews at the command posts, as well as operation and maintenance personnel, literally poured suggestions concerning the system's refinement.

The second stage of the SRF automated command and control system – the *Signal-M* system (mid-1970s through mid-1980s) – already possessed noticeably better characteristics. A mode of automatic connection was worked out in detail at the lowest level and subsequently at training ranges and in troop exercises. Actual missile launches were, as a rule, conducted with the pushing of a button at higher levels – the command posts of a division, army or at the Central Command Post of the SRF and General Staff. This became a type of ritual, crowning many major activities of the military-

industrial complex. The main designers willingly included the higher leadership of the country and of the Ministry of Defense in such remote-control launches. These leaders themselves, more than once, pushed the button. With this goal in mind, regular level 4 *Signal*-M automated command and control equipment was specially installed at the General Staff to imitate the Central Command Post.

Simultaneously, in the command and control system, communications channels of various physical types began to be used – cable, radio, radio-relay and satellite – that essentially heightened the stability of its work in peacetime. At the SRF main staff in the 1970s, a daily accounting of automated system outages for each missile division was conducted. The combined monthly outage time, due to the measures undertaken, was reduced to a few minutes. A new standardized remote command and control system (SDUK), code-named *Pauk* (Spider), was created for the new third-generation silos by the LPI Special Design Bureau. It was extremely protected against unauthorized launches.[121]

Within the framework of the *Signal*-M system, the *V'yuga* subsystem was developed.[122] It was introduced to the troops in 1976-1978, and was used to create supplementary paths for delivering orders to command posts at all levels via broadcast-only radio and satellite communications channels. At a lower SRF level, the *V'yuga* equipment was electrically interfaced with *Signal*-M, in order to allow a remote missile launch to be conducted by radio from the center.

In view of the acceptable operational and technical characteristics of the *V'yuga* subsystem, this development from the LPI Design Bureau was accepted in 1982 for the Soviet Ground Forces, and, with several modifications, for all branches of the Armed Forces.

Additionally, *Signal*-M was interfaced with computer centers of the General Staff, SRF, rocket armies and divisions. This made it possible to accelerate the process of operational re-planning for the use of nuclear weapons, and to solve a number of other computational problems. Later on, members of the LPI Design Bureau developed the information-calculation system, tying all basic SRF computational centers into a unified network.

The most important landmark in the development of SRF command and control has been the creation of the *Perimetr* system. This step was new in principle. Before it, all orders were passed to the missiles via a command post of a lower level, i.e., a regiment or battalion. In the *Perimetr* system, reception of launch commands from the center could be accomplished by radio directly at the launcher.

Here, it is pertinent to step away from a simple listing of the systems developed by the Sokolov group. His engineers, frequently working with the troops, quickly found the key to solving the problem of reliable function of command and control systems in complex combat situations. This key was the communication channels used by the system. One could make outstanding terminal equipment and reliably conceal it in super hardened command posts, but all this would come to naught if the *data transmission channels* were vulnerable.

The experience of using the first generation of automated systems had shown that traditional cables, radio and even satellite communications channels could not support reliable command and control in nuclear warfare or in warfare with massive use of precision-guided weapons. Other means would have to be found. Thus an idea grew for the creation of an independent system of channels for combat command and control, specially intended for extraordinary conditions. Naturally, this could only be radio channels, and hence the system received the designation of radio-combat command and control (*radio-boevoe upravlenie* – RBU). At the installation stage for the *Signal*-M system, several types of such channels appeared, the most important of which became *Perimetr*.

The *Perimetr* system was accepted into service and, since 1985, has been on combat watch. It will be described in the next section. Some types of radio-combat command and control have been described in an authoritative Russian publication.[123] The *Gorn* system mentioned there is a group of *Perimetr* command missiles, based on the SS-20 ballistic missiles. The *Gorn* was on active duty for some time, but then it was retired because the United States and the Soviet Union agreed to destroy ballistic missiles of this class. Several publications provide additional information on the channels of radio-combat command and control.[124]

Finally, the smaller size, weight, and power requirements of this second-generation automated system allowed its accommodation into all command posts of the then new types of missiles. The standardized regimental command posts for remote launch (*otdel'nye starty*) type missile regiments – that is, without any launch crews in the immediate vicinity of the launchers – as well as the mobile command posts of the mobile *Pioner* missiles (SS-20, in NATO terminology), were equipped with the *Signal*-M, *Perimetr* and *V'yuga* equipment. This period demonstrated that, in the nuclear forces, it is impossible to separate the missiles themselves from their command and control system; these, in principle, constitute a unified whole. Hence, the transition from command and control of troops to command and control of nuclear weapons began in the 1970s. This transition was actually completed with the creation of the third-generation automated system – the *Signal*-A.

Signal-A began to reach the troops in 1985-1986. The lowest level of this system – (seventh link) – was installed directly at the launchers, and was an important integral part of them. Without them, not a single new missile could have been put on combat duty. This made the SRF leadership still more attentive to the question of command and control. It is not surprising that in this period the deputies of the SRF commander in chief, and at times he himself, were frequent visitors at the Impuls Corp. Design Bureau, other design bureaus and production plants carefully considering the timetables for testing and production of the automated systems.

The introduction of the *Signal*-A system began also from below, from equipment in the missile complexes (levels 7 and 5) up to the division level and higher. This process has continued even to the present time. The interfacing of the *Signal*-M and the *Signal*-A resources is accomplished at a functional level.

Signal-A allows retargeting of missiles remotely from the General Staff or from the SRF main staff. Several sets of the flight plans (*poletnye zadaniya*) are stored in the equipment of the seventh level (launchers). For retargeting missiles, it is sufficient to indicate in the launch order the number of the corresponding combat plan. Upon receiving the plan number, the automated system gives the command to the missile for the selection of the required flight path, which is carried out automatically within 10 to 15 seconds, after which the missile is launched. Recently, much has been written about retargeting.[125]

The *Signal*-A system comprehensively uses all existing types of "traditional" communications channels and the high-reliability channels of the radio-combat command and control system. It has its own highly secure encryption equipment developed by Impuls Corp., has an improved design and is easy to use thanks to the special minicomputers used by the operators. The extension of this system is being accomplished according to plans, and designers and customers are already looking to the future, where it is proposed to have a *Signal*-Al system. (If, of course, by that time people will not have decided to throw nuclear weapons and all of their excellent infrastructure onto the rubbish heap.)

(C) Development of Command and Control of Sea-Based and Airborne SNF Components

In contrast to the SRF, where creation of an automated command and control system was from the very beginning almost entirely turned over to the military and its research, development and industrial network, command and control of the sea-based and airborne SNF was within the sphere of the general designer of the system for the entire Soviet Armed Forces – Semenikhin (Moscow Research Institute of Automatic Equipment) and once again, of a "general" customer – the General Staff. In the author's opinion, this circumstance had a major influence on the character and tempo of system development for nuclear submarines and strategic bombers.

It is likely that an invisible division of responsibility came about between the General Staff and the main staffs of the Navy and Air Force. But it is even more probable that responsibility was shuffled between them: the General Staff wanted the two services to be concerned with their own systems, while the sailors and airmen figured that since the SNF command and control was strictly centralized in the hands of the General Staff, heirs also were the responsibility of the General Staff. One should keep in mind that the SRF was a brand new service, while the airmen and sailors had their long-standing "attachments" to traditional weapon systems. Therefore, in the Air Force and the Navy, basic efforts in command and control continued to be focused on the non-nuclear portion of the forces, while the concept of the nuclear triad took a second seat. As for the general designer of the Armed Forces automated system, he was, in large measure, preoccupied with such important questions as authorization, protection from unauthorized actions and command and control at the highest level. Hence, he was unable to monitor with sufficient effectiveness the work of his subcontractors –

the command and control systems designers for the different services. Again, perhaps the real reason is different, but the fact remains that development of the automated system for naval and aviation SNF progressed more slowly than in the SRF.

In all fairness, it must be noted that in addition to the indicated organizational reasons, difficulties in solving the problem of reliable command and control for the sea-based and airborne SNF were caused also by technical complexities. SRF sites were deployed in rigidly fixed areas and were literally dug into the ground. Therefore, from a technical point of view, their command and control was based on cable communications channels within the country. Even radio and satellite communications were established more easily along well-developed permanent routes. Conversely, submarines and strategic aviation, as a basic mode of duty, patrol regions remote from the center. Moreover, a constant major obstacle for reliable delivery of orders to deeply submerged boats was the thickness of the water, which, as is known, can be penetrated only by VLF transmissions.

Sea-Based SNF

When the first missile-carrying submarines (SSBs or SSBNs) joined the Soviet Navy in the early 1960s, their command and control was not different in principle from that of conventional submarines. The main difference was the General Staff's monopoly on planning the use of strategic nuclear weapons on-board, and implementation of launch operations. The rest of the routine control and combat duties were the responsibility of the Navy staffs.

Under the leadership of the Moscow Research Institute of Automatic Equipment, the Design Bureau Mars in the city of Ul'yanovsk, headed for many years by V.V. Alekseychik, carried out development of automated command and control systems for sea-based SNF. The main enterprise for serial production was the Research and Production Association *Komintern*, in Leningrad.[126]

During the initial period of SSB/SSBN operation by the Soviet Navy, their command and control was based on the same "packet" principle as the SRF command and control. Emergency orders to change the alert status and to carry out the assigned missions were transmitted from the General Staff or the main naval staff using the Monolit system and operational radio networks. The orders were delivered to the submerged SSB/SSBNs by means of powerful stationary VLF transmitters located throughout the Soviet Union. Six known transmitters within the vicinity of the following cities were most often used: Krasnodar (*Gherakl*), Gorky (*Goliaf*), Arkhangelsk (*Atlant*), Frunze (*Prometey*), Khabarovsk (*Gherkules*) and Molodechno (*Antey*).[127]

Arctic ice did not interfere with the underwater reception of orders in the VLF range. In the Arctic Ocean, a series of exercises with real ballistic missile launches was conducted. Having received the order, the submarine surfaced, broke through an ice crust of up to two meters thick, and conducted a launch. After reporting mission accomplishment to the center by a short-wave broadcast, it submerged.

The transition to automatic command and control of the sea-based SNF happened at the same time that, as described above, the Armed Forces introduced its automated system as a whole in the second half of the 1960s. The fundamental problems at this stage were strengthening protection against unauthorized actions by a submarine crew member; the expansion of operational capabilities of command and control; and improvement of survivability and of radio channel capacity, which was supposed to reduce the submarines' time on the surface.

The communications channels gradually improved. From the end of the 1970s, a satellite communications system, which has a greater noise-immunity and capacity than old HF communications, began to be used for two-way communications sessions with surfaced submarines. The radio lines were fully secure. Antennas were improved for reception in the VLF and ELF ranges while submarines were in submerged movement. The tethered-type antennas, several kilometers long and towed behind a moving submarine, produced satisfactory results as a whole. Antennas towed by modern submarines enable them to receive communications while at working depth. In addition to radio communications, submarines can use acoustic communications; its main advantage is that submarines do not need to surface and use retractable and towed antennas. However, since the range of underwater acoustic communications is short (not more than 10-30 km), it can be used only in some cases, for instance, when surface escorts accompany submarines.[128]

With the delivery of the first KSBU models to the Armed Forces, their prototypes began to be installed and checked at fleet and SSBN division command posts. However, the beginning of their official combat use should be considered 1985 – the year KSBU was accepted for combat duty.

In spite of some achievements in improving the sea-based SNF command and control system in the 1970s and 1980s, the rather high vulnerability of its ground elements, i.e., the command posts and shore communication facilities (*beregovye obyekty svyazi*) of the fleets, and also the relaying radio transmitter centers, remained a major deficiency.

To remedy these shortfalls, several measures were undertaken. Several mobile command posts and truck-mounted HF transponders, and also a group of VLF-range *Orel*-type relay aircraft based on the TU-142mr, were introduced into the sea-based SNF command and control system.[129] However, the mentioned steps, in the opinion of a number of experts, gave only an insignificant increase in command and control reliability. The *Orel* capabilities for long-range operations proved to be significantly lower than those of the American TACAMO system, and the mobile command posts were bulky and not particularly mobile. More decisive actions for improving submarine command and control were not taken because of a Soviet tendency to underestimate the sea-based component of the nuclear forces.

When the Russian leadership, according to START II, agreed to a sharp reduction of land-based ICBMs, questions concerning the command and control of the sea-based SNF took on a different meaning. According to that agreement, by 2003-2005 more

than half of the Russian strategic nuclear warheads could be carried by submarines. Therefore, the issue of strengthening reliability of submarines command and control was taken into account in Russia during the process of START II ratification and in considering subsequent reductions of strategic offensive weapons. A rather complete description of command and control of Russian sea-based SNF can be found in a recent book, and in its bibliographic material.[130]

Airborne SNF

The creation and development of a command and control system for the airborne SNF also encountered several complex problems, mostly in the area of providing reliable communications with strategic bombers patrolling far away from their ground bases.

The development of a command and control system for strategic bombers was overseen for many years by the Research Institute of Mathematical Machines in Yerevan (Armenia); the chief designer was Robert Atoyan. Series production was organized at the *Elektron* assembly plant, also in Yerevan.

Initially, combat orders were transmitted to the strategic bombers only by means of HF radio channels, which have weak noise immunity especially in the northern regions, close to the territory of the potential opponent. In the 1970s, long-range aviation was equipped with satellite communication stations, which somewhat improved its command and control. Work is being conducted to equip the TU-95M and TU-160 bombers with *Perimetr* receivers, which is viewed as a sufficiently effective measure to improve command and control of airborne SNF.[131]

4.2 Russian Strategic C³ Today

4.2.1 The Highest Level of SNF C³

The Russian president has the right to authorize use of nuclear weapons. The highest level of C³ includes, in addition to the president, the minister of defense, the General Staff, and the commanders in chiefs of the SRF, Navy and Air Force.

Organization of the development, production, storage and maintenance of nuclear warheads of strategic weapons is entrusted to a special structure within the Ministry of Defense – the 12th Chief Directorate. This directorate is subordinated directly to the minister of defense, and has its own storage facilities, as well as special subunits within the nuclear triad. These subunits' specialized functions are subordinated to the 12th Chief Directorate, while operationally and administratively they are under the commander of the respective SRF, Navy or Air Force unit.

To ensure that all three legs of the nuclear triad function normally, they constantly work together with the other elements and structures of the Russian Armed Forces.

In order to provide for continuous command and control of the troops in general, and especially of the nuclear forces, a system of command posts has been deployed and is operational. The highest level command posts include:

- underground, super hardened command posts in the city of Moscow, and the Moscow region (Chekhov);
- airborne command and control posts for the General Staff, the SRF, the Navy and the Air Force, based near Moscow;
- railroad and mobile ground (truck-mounted) command posts.

These command posts are connected by two-way communications channels, and are equipped to receive an EWS signal of a nuclear attack. There is also a system for one post to take over from another.[132]

Individuals and agencies included in the higher level of SNF C^3 are continuously connected to each other by a special communications system, *Kazbek*. (Fig. 35) This system includes:

- portable equipment (*Cheget*) used by the president to prepare and issue authorization for the use of nuclear weapons (the "nuclear briefcase");
- terminal equipment (*Baksan*) installed at command posts of the General Staff, SRF, Air Force and Navy to receive the president's authorization;
- the special communications system *Kavkaz* (radio, radio relay and satellite communication channels). This system connects the "nuclear briefcase" to the *Kazbek* network from wherever the president happens to be, and delivers information to all *Baksan* devices with necessary reliability, security and speed.[133]

The "nuclear briefcase" outwardly does not differ from a typical hard-shell briefcase. The designers manufactured several samples, but how many "briefcases" were really used in the Soviet SNF command and control is unknown. Some believe that three were used for preparation and release of nuclear authorization: one belonged to the general secretary of the Communist Party's Central Committee, one to the minister of defense, and one to the chief of the General Staff. A clear, official description of this complex and crucially important process does not exist. The situation is similar in the United States.

The widely held opinion that *Cheget* is the same "nuclear button" with which the president can launch strategic missiles is erroneous. The launch of a missile is impossible without the military, starting with the crews at the command posts of the General Staff. The authorization of the president is no more than the permission and order to launch.

The special communications system of the national leadership, *Kavkaz*, has a high survivability in crisis conditions thanks to being based on a wide, mutually-connected network of cable, satellite, radio and radio relay two-way secure channels of communication. Wherever *Cheget's* operator might be, he can connect it to this network and transmit authorization to the General Staff's Central Command Post. The *Kavkaz* system simultaneously supports communication between senior government officials while they are making the decision whether to use nuclear weapons, without requiring them to be gathered in one place.

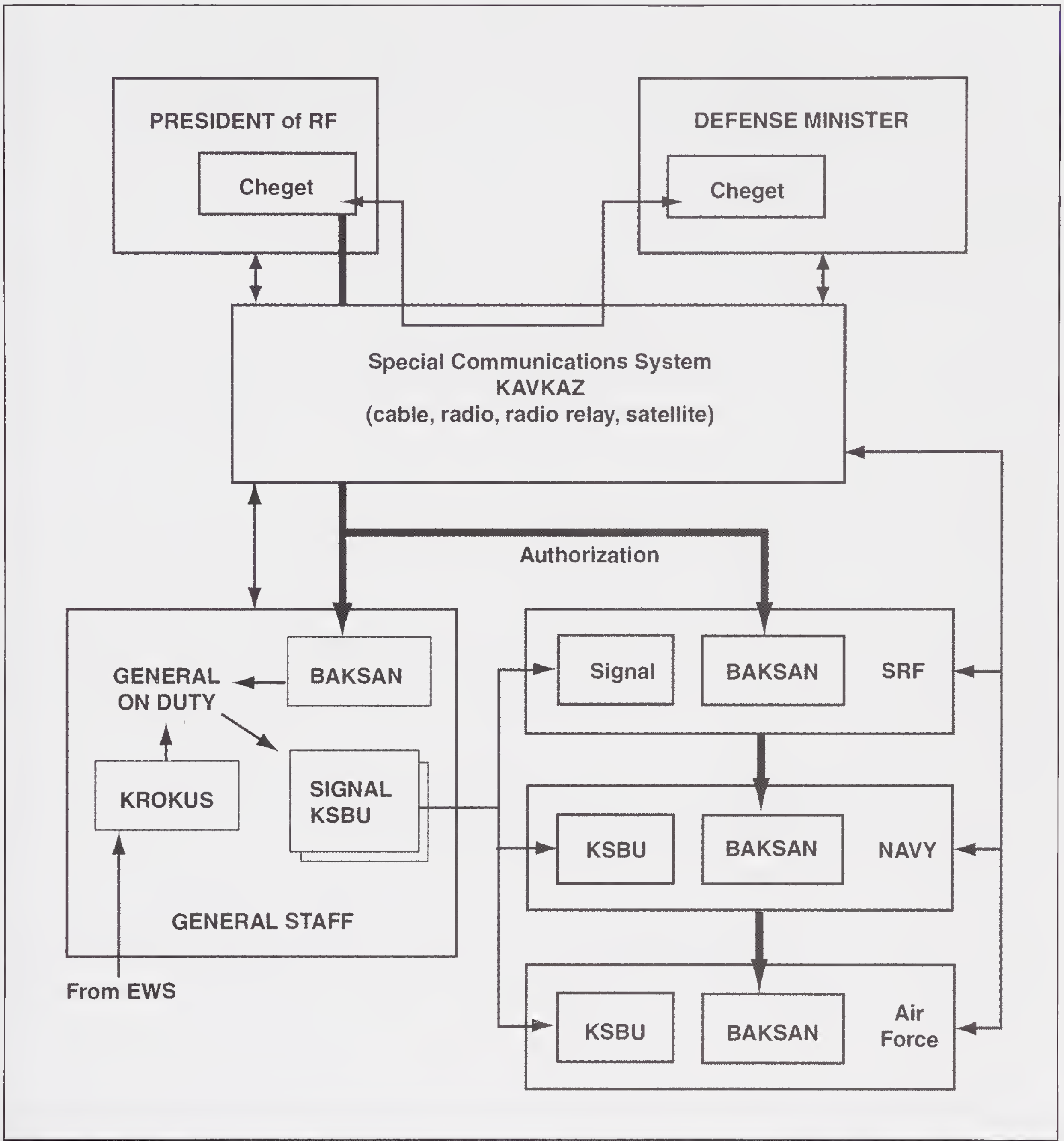


Fig. 35: "Kazbek" system.

Baksan equipment has been installed at all General Staff command posts. Once official authorization has been received by the *Baksan* equipment and verified via other channels, the General Staff crew must begin to carry out the order. *Baksan* has also been installed at all of the SRF, Air Force and Navy command posts in order to monitor the situation and for expediting preparatory operations.

Another high-level technical resource for SNF command and control is the *Krokus* display, the terminal receiving equipment for the missile attack warning system. Data arriving at *Krokus* is verified through a special procedure and expedites those prepara-

tory operations that may be conducted up to the receipt of authorization.[134]

KSBU is a combination of special computers installed at Armed Forces command posts (other than the SRF), interconnected by various channels and a unified algorithm. It allows transmission of orders, the reception of reports, and is interfaced with computer centers and the *Signal* system. There is an around-the-clock duty watch at KSBU consoles. [135]

Duty crews at the highest level command posts continuously monitor the condition of nuclear missiles and troops, and receive reports about accidents on a level appropriate to the importance of the accident. Attempted unauthorized actions within the command and control system or with nuclear weapons are automatically reported through all levels up to the Central Command Post of the General Staff. Everything and everybody are in constant readiness to prepare and issue orders to the troops to unblock and launch the missiles.

The work algorithm of the Russian SNF's highest level of command and control corresponds to the general principle of C^3 systems architecture as described in Chapter 1. Once the warning of a missile attack is received and its source identified at the command posts of the General Staff and the services armed with strategic nuclear weapons, a report is sent to the president and the minister of defense. Depending on the unfolding situation, and in accordance with the current concept of retaliation by the SNF, authorization to use nuclear weapons is transmitted via the *Cheget* equipment to the highest level of the Armed Forces' command and control. Launch orders are prepared at these command posts, and then are transmitted to the troops simultaneously using all available technical means – KSBU, *Signal*-A, *Vyuga*, *Perimetr* and others.

According to the information provided by a Soviet expert on negative control during U.S. Senate hearings in September 1991,[136] protection of the Soviet nuclear command and control system against accidental or unauthorized actions was based on the following principles:

- rigid centralization at the highest level over the decision to use nuclear weapons and issue execution orders to the troops;
- essentially equal and sufficient protection against unauthorized actions in all the three legs of the nuclear triad;
- increasing level of protection from lower to the higher levels of command and control.

Russia's SNF C^3 system continues to function along the same lines, and completely excludes any possibility of a launch performed by one person.

The crew at the General Staff's command post directly commands the nuclear triad's troops in launch preparation and actual launching of the missiles. According to the mentioned Soviet C^3 expert, the whole process of combat command and control can be divided into four stages.

The chief of the General Staff and the corresponding commander in chief send the

preliminary command to the troops after the first information about an attack comes from the EWS. This order automatically switches the command and control equipment at all levels from watch duty to combat duty, and allows the crews at command posts access to launch equipment and operational documents. However, at that time the crews are capable only to carry out some preparatory steps, but not to launch the missiles.

The *permission command* is issued upon final confirmation of a missile attack against Russia. The president, minister of defense and chief of the General Staff together prepare the authorization for use of nuclear weapons. It is sent to the three commanders in chief, and delegates launch authority to them.

The *direct command* is prepared by the chief of the General Staff and by the commanders in chief and is sent to the action levels as an order to launch the missiles. (We are talking not about actions by an individual, but by appropriate combat crews at the command posts of the General Staff and main staffs of the services[137].) The crews at the action level verify it with the help of special organizational and technical methods. After receiving this command, which also contains the unblocking code value and the number of the operational plan, the crews at the lowest level of the C^3 system are physically enabled to launch the missiles. Each launcher automatically receives concrete targeting data depending on the number of the operational plan contained in the direct command.

The action crews issue the *launch command* directly to the weapons themselves after the direct command is verified. This operation is limited to a very short period of time, after which the channel for transmitting the command is switched off.

Finally, the last barrier to launch is an automatic verification of the command in the launcher itself. If the result is positive, the missile is launched.[138]

The description provided by the Soviet expert in 1991 should also include the capability to launch missiles without participation of intermediate and low levels in the chain of command, using *Signal*-A and *V'yuga* (order transmitted electrically via regimental command posts), as well as via *Perimetr* (by radio signal directly to launchers).[139]

One should emphasize once again the rigidly centralized character of the SNF C^3. Not a single missile with a nuclear warhead can launch until the highest level Command Post releases a specially guarded unblocking code value, nicknamed *goschislo* (*gosudarstevennoe chislo* – state number).

4.2.2 SRF C^3 System

(A) ***The Technical Means For Command and Control From the Center***

Signal-A

The main technical means for command and control of the SRF is *Signal*-A, which includes the subsystem *V'yuga*. (See Fig. 36)

Signal-A routinely monitors the condition of nuclear missiles and troops, changes in their state of alert and preparation for missile launches. This system's equipment is installed at all command posts and directly in the launchers, from the General Staff down to the stationary and mobile ICBMs.

The system has several modes of operation. The main operational mode is the automatic electronic interface of all levels of command and control into an integrated network, by which missiles can be launched directly from the command posts of the General Staff, exclusive of the intermediate level command crews. In this case, the launch command follows all the descending steps of the hierarchical ladder, but the intermediate level acts only as an automatic relay station, while the combat crews are observers. There is also a manual interface mode, which allows one level to launch its "own" missiles. This operational mode can be introduced only by special command from the General Staff, upon receipt of which the *Signal*-A console at a given level's command post is unblocked. There is also a mixed mode of operational interface.

Signal-A is very fast. A command from the General Staff reaches the ICBM launchers not more than 30 seconds after it was given. According to Yakovlev, the former SRF commander in chief, "the SRF officers still remember how the then Minister of Defense Army Gen. Pavel Grachev, when visiting the Central Command Post of SRF, attempted to give them a dressing down for 'brazen bluffing' – the computer monitors at the Central Command Post automatically provided new information on the combat readiness of each missile in the SRF units."[140] The collection of reports from all subordinate levels and the appearance of this generalized data on the displays at the Central Command Posts takes no more several minutes.

The highest levels of *Signal*-A interface with computer centers are capable of large-scale calculations, such as the correction of operational plans for SNF combat use or calculations of new flight missions for individual ICBMs.

The reliability of the system is guaranteed by the use of several independent, widely dispersed (physically) communication tracks for each pair of levels. Each communication track may have several channels of a different physical nature – cable, radio, satellite, tropospheric, etc. The switch from a damaged channel to a backup one is done automatically within several seconds. All the channels are highly secure.

Since the *Signal*-A system is characterized by redundancy, it is highly reliable and combat-ready on an everyday basis. Over many years of operation, there has not been a single, even minimally serious case of disruption in communications between the command posts of the General Staff, the SRF commander in chief and the ICBM launchers. The system's improvement is ongoing in order to strengthen its stability and expand its combat potential.[141]

As noted earlier, *V'yuga* is a part of *Signal*-A. This redundant system, using HF, VLF and satellite communication channels, serves for one-way radio transmission of launch orders and other commands to the troops. All command posts, including regimental ones, are equipped with *V'yuga* receivers. Working HF frequencies are selected individually for each area of reception, based on optimal conditions for the propagation of radio waves in that given area. Therefore, the system has a number of territorially dispersed radio transmitters, which are controlled in synchronism from one high level command post operational at that given moment.

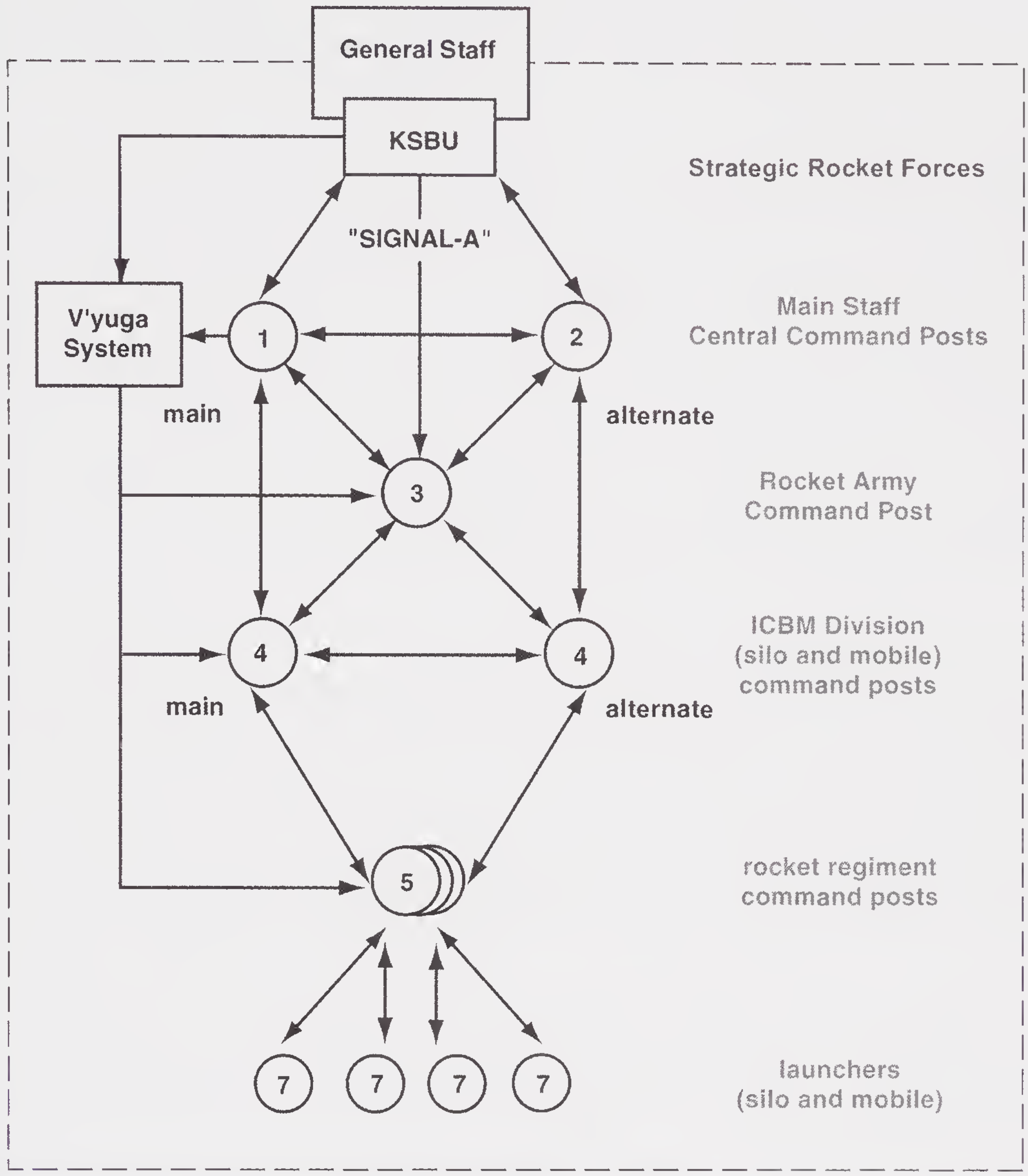


Fig. 36: "Signal-A" system.

Signal-A and *V'yuga* are interfaced electrically and algorithmically, and are used simultaneously.

Despite the high everyday reliability of the system described, the Russian military command and other experts believe that it must be supplemented by some means that will guarantee reliable delivery of launch orders to missiles under the extraordinary conditions of nuclear war. Hence, from the late 1970s onward, the Soviet Union began to develop a backup SRF command and control system. At the same time, *Signal*-A came to be referred to as the main SRF C³ system.

Perimetr

This backup system of the SRF command and control was specifically designed and developed for conditions of nuclear war. All its nodes and channels are especially survivable. Its main element is a system for transmitting launch orders under extreme conditions using *Perimetr* command missiles.

The world mass media began to pay attention to *Perimetr* (nicknamed "Dead Hand" in the West) in the early 1990s, and since that time most that has been written on the subject is erroneous, incomplete and sometimes distorted on purpose. There have also been some relatively serious publications.[142] It was only in 1999 that Russia officially recognized the existence of *Perimetr*. One of the most important documents in this respect is *The Russian Strategic Missile Complexes*, edited by members of the Russian Academy of Sciences, V.F. Utkin, Y.S. Solomonov and G.A. Yefremov.[143] The foreword to the book was written by Gen. V.A. Subbotin, chief of the SRF Rocket and Space Armaments. The following is an excerpt form the book:

> "*The Missile complex 15PO11 "Perimetr" ("Perimetr-RTs") with the missile 15A11.* The development of the draft design of the command missile of the Perimetr system was ordered by the decision of the Central Committee of the CPSU and the Council of Ministers of Aug. 30, 1974. The method of combat command of military facilities under extreme conditions utilizing command missiles was proposed by Chief Designer V.F. Utkin in conjunction with other experts. In December 1975, the draft design of the system was completed; the specialized equipment was developed by the OKB LPI [Special Design Bureau of the LPI]. In December 1977, the draft design of the command missile 15A11 with nose cone 15B99. In December 1978, the first launches of the missile 15A11 were conducted in order to test specialized equipment and improve the system for issuing commands for missiles launch during the special period. The flight testing of the command missile 15A11 was completed in March 1982. In January 1985, the complex of the command missiles of the Perimetr system was put on combat watch.
>
> - The designer – Design Bureau "*Yuzhnoe.*"
> - General Designer – V. F. Utkin.
> - Manufacturer – *Yuzhnyy mashinostroitel'nyy zavod.*
> - Classification according to START I – assembled ICBM in a launch container (Class A).
> - The type of the complex – strategic missile in the silo of remote launch type, with a third generation command missile.
> - Status – on combat watch since January 1985, passed acceptance tests in December 1990.[144]
> - Missile – 15A11
> - Nose cone – 15B99[145]"

The history of development and introduction to combat duty of the *Perimetr* system is described in sufficient detail in the *Military Encyclopedic Dictionary* of the SRF, in "The Chronology of the Main Events in the History of SRF."[146] Information on the mobile version of the command missiles of the *Perimetr* system, based on the Topol ICBM, has also been published.[147] SRF experts consider Col. Gen. Varfolomey Korobushin to be the father of *Perimetr*; he led a large group of military officers and civilian specialists throughout the system's development, testing and introduction to combat duty.

The crucial characteristic of *Perimetr* is its ability to transmit an order from the General Staff directly to the ICBM launchers, physically bypassing (in contrast to *Signal-*A) all intermediate command posts of the SRF.

The principle of the system's operation is as follows. During the threat period, facing a possible enemy attack, several previously selected officials (at the level of deputy minister of defense, or equivalent) move into a special, super hardened underground facility in the vicinity of the main command post. This facility, referred to as the radio command and control center, is equipped with a powerful LF and MF transmitter, as well as with an underground antenna, as super hardened as the facility itself.

Imagine the following, purely hypothetical, scenario. The EWS display at the Central Command Post of the General Staff shows information warning of an enemy missile attack. This is a unique situation, without anything analogous in the history of humankind. The people at the command post, be it the president or duty crews, are facing Hamlet's choice: to be, or not to be? – To issue an order for a retaliatory nuclear strike, or not? It is easy to imagine that a mistake, i.e., a positive response to false initial information, would have much more horrible consequences than in the case of the Prince of Denmark.

For many years both the Soviet Union and the United States came, with surprising ease, to the same certainty: a warning of a missile attack by the EWS should initiate an *immediate* retaliatory nuclear strike, or it might be too late. Operational documents say this even today, and such an approach governed all the concepts for building C^3 systems and the strategic offensive forces themselves (with corresponding huge expenditures).

The spirit of the Cold War itself could explain, to a certain degree, this conclusion. But today it is becoming increasingly obvious that such a concept drives into a dead end the people whose duty it is to be supremely cautious and ultimately responsible in critical moments; that it denies them their right to make a mistake.

The super hardened element of the *Perimetr* system, described above, mitigates the critical nature of that choice. Upon receiving a warning of a missile attack (a warning which, in theory, can be false) the NCA has an opportunity to temporarily switch the responsibility for this unique decision over to authorized individuals who may stay alive after the leadership itself has perished. It is critically important that this surviving crew can carry out its combat orders only after receiving confirmation of actual nuclear detonations on Russian territory and if the leadership has perished or cannot, for technical reasons, carry out its duties at the main command post.

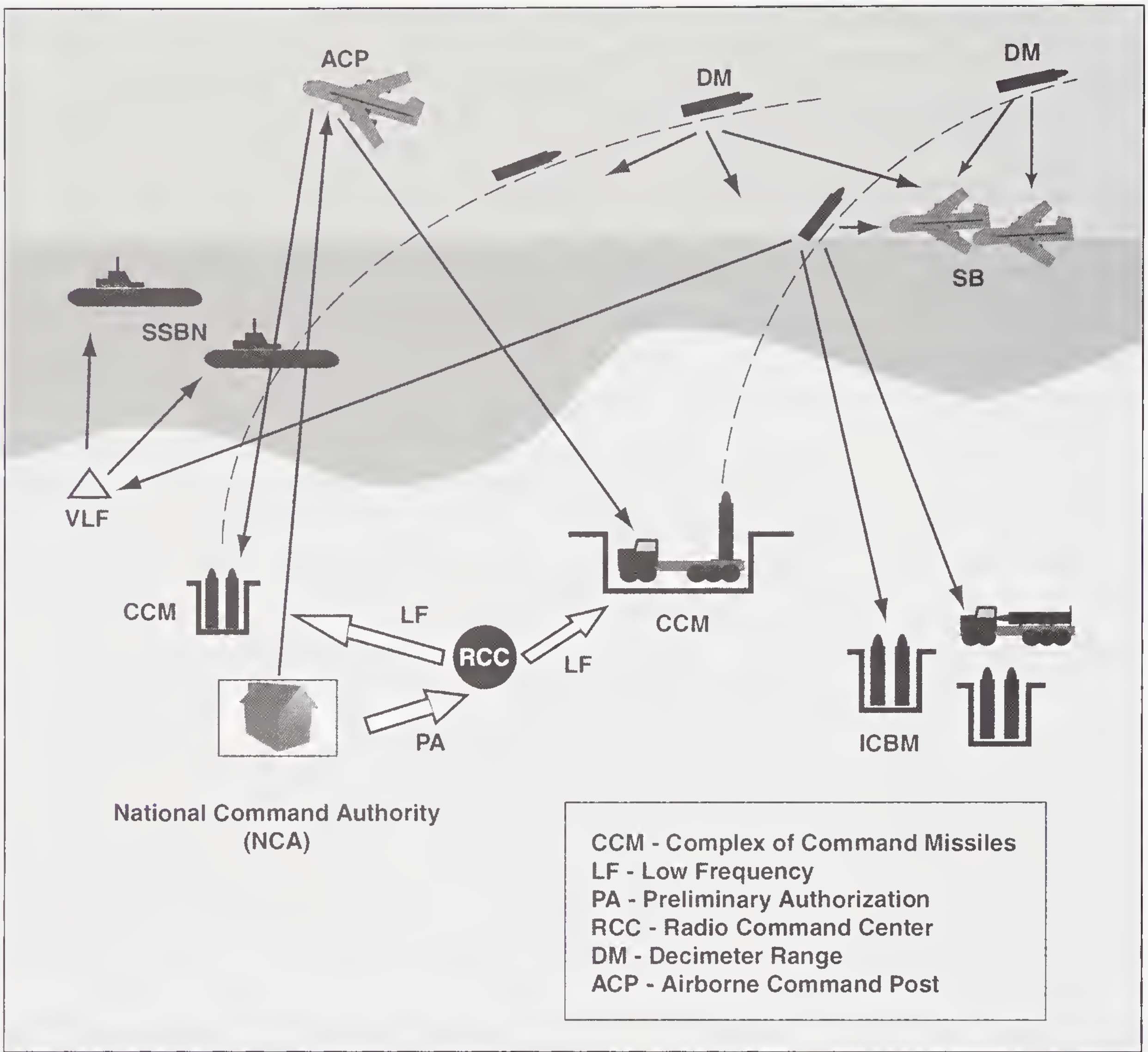


Fig. 37: "Perimetr" system.

Technically, this is made possible when the NCA transmits a special code for preliminary authorization to the super hardened radio command and control center. The crew working at the center can prepare and transmit the launch order to the troops only if three conditions are simultaneously met: the release of preliminary authorization, a complete loss of communications with the NCA, and reception of reliable information about nuclear detonations from different types of sensors (visual, seismic, etc.). The system has no capability for preparing a launch order automatically without participation of the center's crew. If, with a certain period of time, there is no evidence of actual nuclear explosions, the system returns to its initial status.

Since the transmission range of the underground antenna in the radio command and control center is limited, the *Perimetr* system can relay the launch order via command missiles. Stationary and mobile launchers for these missiles are located within range of the center's radio channel. Upon reception, the order is automatically recorded into

the nose cones of these command missiles, which are equipped with special radio transmitters instead of nuclear warheads. The missiles are then launched along pre-selected trajectories over Russian territory and, during the entire flight, transmit the launch order to armed missiles, as well as to command posts at every level.

To put it briefly, *Perimetr* has two crucial advantages: it reduces the probability of a tragic mistake and it increases the probability of retaliation. Its shortcomings include a relatively slow speed of operation, since it takes 35 to 40 minutes to transmit the launch order to those armed missiles located at the greatest distances from the center. This means that while a Russian retaliatory strike would be highly probable, its size (the number of missiles launched) may turn out to be comparatively small. But the relativity of the concept "comparatively small" in any given case will be addressed below, in an analysis of various concepts of SNF retaliation.[148]

(B) The Division Of Silo-Based ICBMs

The architecture of C^3 for a division with silo-based ICBM regiments is seen in Fig. 38.

An ICBM division's command has two stationary hardened command posts, the main one and a reserve, as well as a mobile, automobile-based reserve command post, and a helicopter-based airborne post. There is a procedure for passing the command and control from one post to another, as necessary.

The stationary and reserve command posts of the division are connected with one another by several branches of underground communication cables, each one encompassing from one to three highly-protected, underground standardized command posts for missile regiments. These cable channels are used for round-the-clock operation of the *Signal*-A system, as well as for routine administrative telephone and loudspeaker communication.

Direct cable lines connect a missile regiment's standardized command post to each of its silo-based launchers. The cables are designated for continuous detailed monitoring of the missiles' technical condition at the regimental post (and more generally, at divisional and even higher command posts). These same cables are to be used to transmit combat launch orders to the missiles. Silo-based launchers have no crews, and only external guard teams are located near them. All launch equipment and the ICBM itself are remote-controlled from the standardized command post of the missile regiment.

The command and control system of the missile division is hardened against the impact of nuclear and conventional weapons, as well as electronic jamming. The cable lines are backed up, in case of damage, by radio relay and radio communication channels. Some launchers of neighboring regiments are connected with cables in a way that forms a common network for divisional command and control. In an extreme situation (and, obviously, only after receiving special orders from above), this permits launching all of the division's ICBMs from any one standardized command post of a missile regiment. In other words, each regimental standardized command post can be used as the division commander's command post. This is a substantial advantage because of the

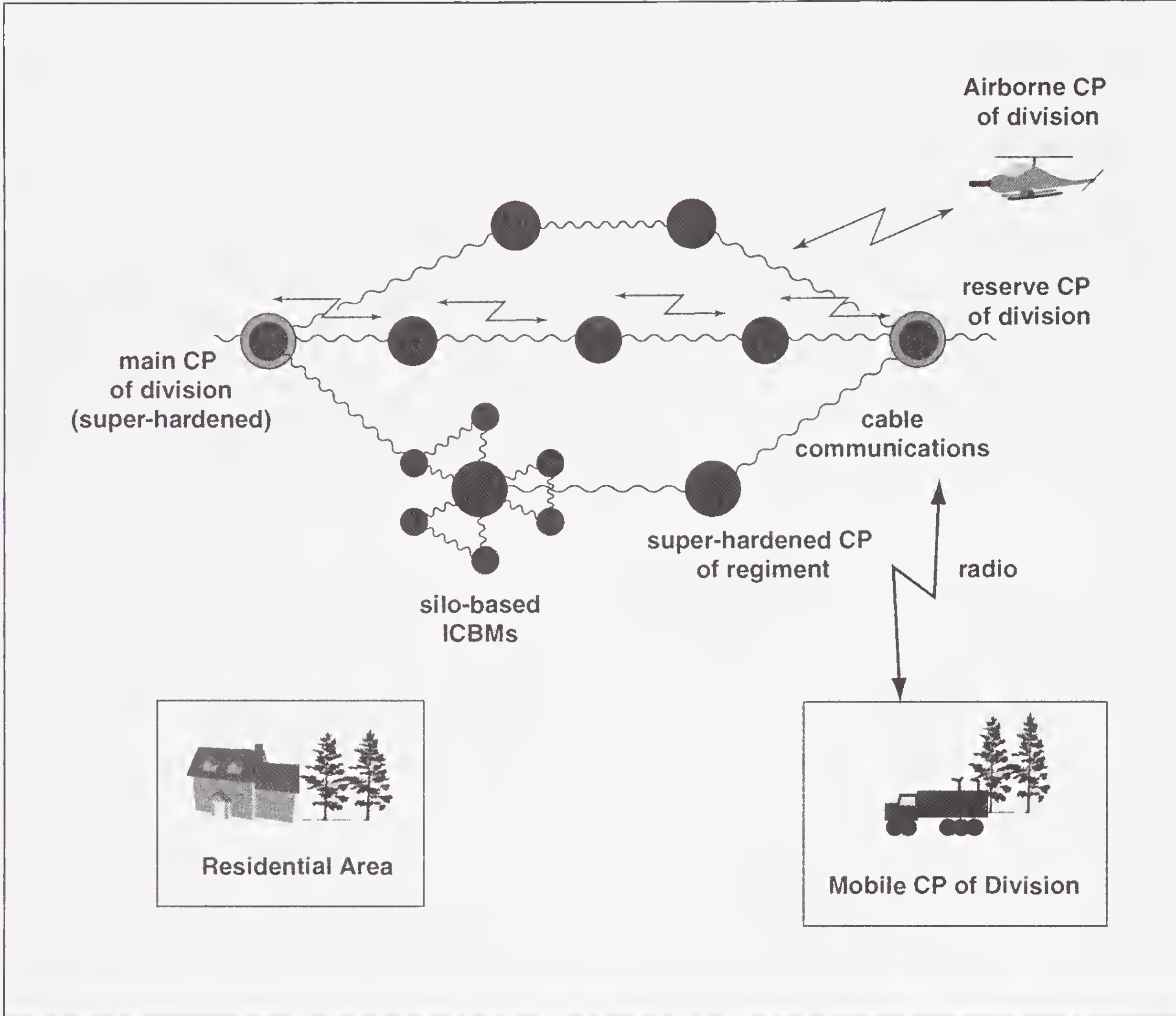


Fig. 38: Silo-based ICBM division.

possibility that a considerable portion of divisional and regimental command posts would be destroyed by a nuclear or massive conventional strike.

The reliability of combat order transmissions is further guaranteed by the flexible technical capabilities of the division commander's regular command posts: the main post, the reserve post, the mobile reserve post and the airborne post. All of them have independent channels for receiving information from the higher levels (including *V'yuga* and *Perimetr* receivers), as well as independent direct radio channels for the transmission of launch orders to the silo-based launchers.

Finally, the most important measure to increase the survivability of the command and control system of an ICBM division is not only its hierarchical architecture, but also the capability to transmit orders from above directly to the regimental command posts and to the launchers, bypassing the division command. This is achieved by equipping all missile regiment command posts with *V'yuga* and *Perimetr* receivers, and launchers with *Perimetr* receivers.

A number of other measures to strengthen the reliability of divisional command and control under extreme conditions have been implemented.

As one can see, the missile division's C^3 system has a wide range of technical means that give it considerable flexibility in both combat command and routine activities. These technical means are operated in a manner determined by the General Staff and the SRF commander in chief.

(C) Command And Control of Mobile ICBMs

The C^3 system of an SS-25 (*Topol*) mobile ICBM division is shown in Fig. 39.

The principle of mobile missile C^3 is largely similar to that of a division of stationary

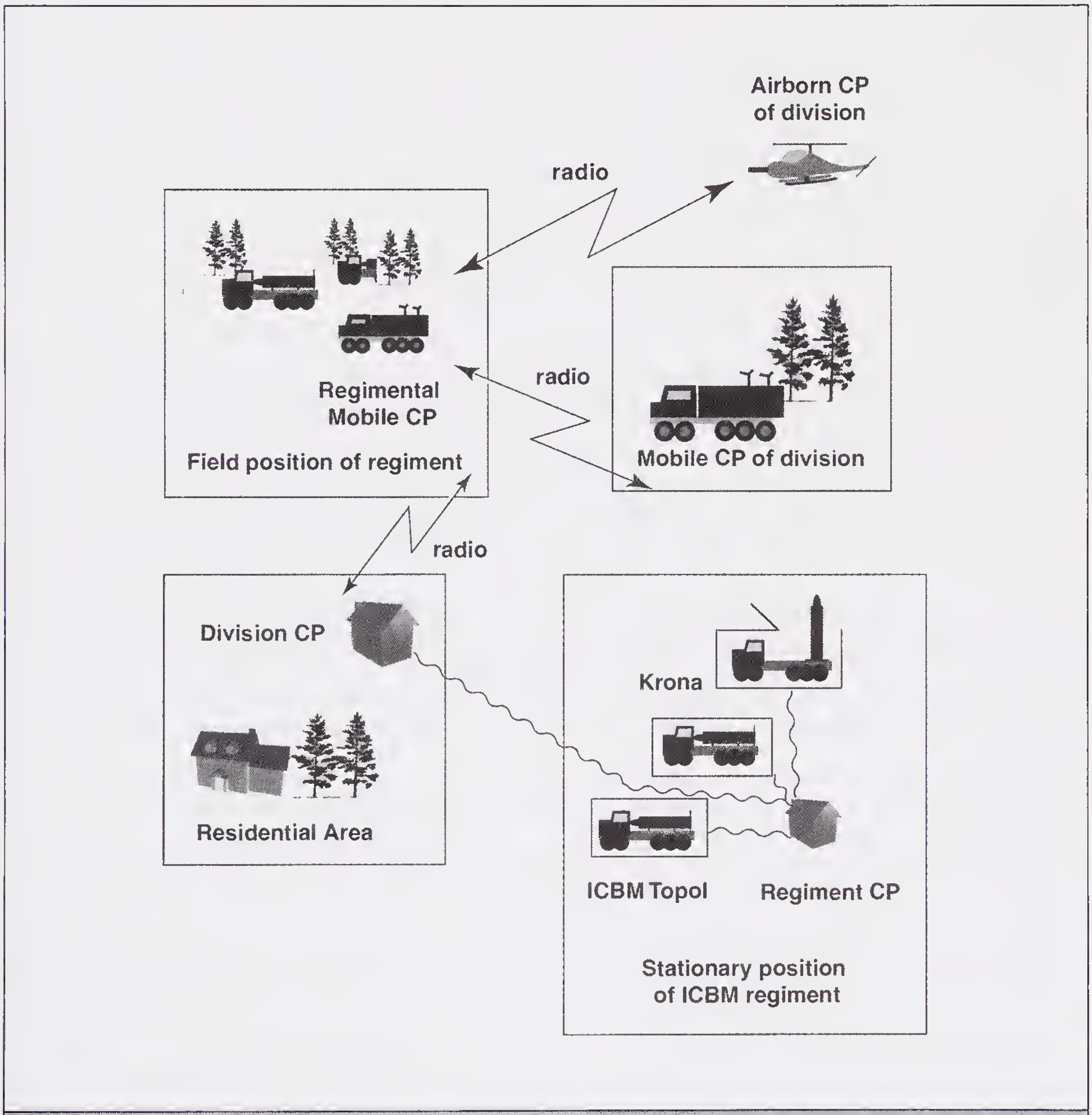


Fig. 39: Mobile ICBM "Topol" division.

ICBMs. It also combines a hierarchical structure with direct channels from the highest levels of command and control down to the launchers. The division command has approximately the same set of command posts. The channels of combat command and control are also sufficiently redundant. At the same time, there are a number of differences, determined by the special character of the mobile ICBMs' operation.

The regimental command posts are mobile, like the ICBMs themselves. Unlike silo-based launchers, mobile ICBMs require service crews, which include, in addition to the guards and drivers, personnel that are able, under certain conditions and with authorization, to launch the missiles. When these regiments are deployed in the field or are in motion, their C^3 depends almost entirely on radio. Cable communication can be used to a limited degree only if there is a communication center in the vicinity of the field position.

Under combat conditions the autonomous launchers on the march use UHF channels to maintain continuous operational telephone communication with their regimental command posts. They are also constantly ready to receive launch orders via the *Signal*-A system, and directly from the highest levels of command and control via the *V'yuga* and *Perimetr* systems. Once the launch order is received, the mobile ICBM command deploys in the field and executes the order. The flight mission is entered without the participation of the crew, i.e., automatically in the course of the launch procedure, in accordance with the information contained in the launch order.

Since it is necessary to save the ICBM transporters from excessive use, the mobile SS-25 regiments spend much of the time in the areas of their permanent bases. They deploy to their field positions according to training plans or in a period of real threat. However, the long-existing concept of a surprise nuclear war predetermined a variant of combat watch for the mobile ICBMs at their stationary positions.

At their permanent regimental base, mobile SS-25 ICBMs are stationed in special, unprotected structures with *Krona* retractable roofs. The mobile regimental command post is located nearby in a similar structure. There is also an unprotected stationary building for the regimental command post, fitted with C^3 equipment. All these structures have the necessary antennas and are hierarchically connected with cable lines to the higher levels.

Constant combat watch is carried out either in the stationary command post building, or directly in the mobile command post's vehicles, parked in their facility. Upon receiving of combat orders, ICBMs are launched from the *Krona* facilities automatically. The launch can be implemented by remote control from the center or by the crew at the regimental command post once they receive authorization. This variant in the launch control is determined by the duty established in the *Signal*-A system based on the directive by the General Staff or the SRF commander in chief.[149]

The SRF commanders in chief and their deputies paid constant attention to command and control, and made considerable contributions to the improvement in SRF C^3.

SRF Commanders in Chief – Deputy Ministers of Defense

- Mitrofan Ivanovich Nedelin, chief marshal of artillery, Hero of the Soviet Union – 1959-1960
- Kirill Semenovich Moskalenko, marshal of the Soviet Union, twice Hero of the Soviet Union – 1960-1962
- Sergei Semenovich Biryuzov, marshal of the Soviet Union, Hero of the Soviet Union – 1962-1963
- Nikolai Ivanovich Krylov, marshal of the Soviet Union, twice Hero of the Soviet Union – 1963-1972
- Vladimir Fedorovich Tolubko, chief marshal of artillery, Hero of Socialist Labor – 1972-1985
- Yury Pavlovich Maksimov, Army general, Hero of the Soviet Union – 1985-1992
- Igor Dmitrievich Sergeev, Army general, 1992-1997
- Vladimir Nikolaevich Yakovlev, Army general, 1997-2001
- Nikolai Yevgen'evich Solovtsov, colonel general, 2001-current

First Deputies of the SRF Commander in Chief

- Vladimir Fedorovich Tolubko – 1960-1968
- Mikhail Grigor'evich Grigor'ev – 1968-1981
- Yury Alekseevich Yashin – 1981-1988
- Aleksandr Petrovich Volkov – 1988-1994
- Nikolai Yevgen'evich Solovtsov – 1995-1997
- Anatoliy Nikolaevich Perminov – 1997-2000

In 1999, Yakovlev initiated the creation of a unified information and reference system of the SRF local area network. The system embraces all aspects of life of the SRF, from combat readiness to finances and logistics. Using his personal computer and the equipment of the SRF Central Command Post, the commander in chief can at any moment receive all the information he needs, be it the deployment of a Topol ICBM to a firing position, the availability of fuel and lubricants in a regiment, or the number of patients in the SRF Central Hospital. This system proved to be very useful when optimizing distribution of limited resources and organizing the operational and financial plan of repair work by the industry and by the missile depots. Of course, the need to collect, process and transmit huge amounts of data has required a lot of additional work from staffs and combat crews of command posts. But according to Yakovlev, this has allowed, despite all the difficulties, to maintain the index of SRF combat readiness at the very high level of 0.95.[150] In addition – and this is quite important – such an all-seeing eye facilitates prevention of unauthorized actions within the C³ system and with the weapons themselves.

4.2.3 Command and Control of the Sea-based and Airborne SNF

The main technical means for transmitting General Staff's orders to SSBNs is KSBU, the system of combat command and control. The organizational and operational principles of this system are largely similar to *Signal*-A, which is used by the SRF. All levels of the sea-based SNF command and control have KSBU equipment, including the General Staff, the main naval staff, and subordinate staffs. SSBNs themselves are equipped with special devices interfaced with KSBU at the higher levels.

The survivability requirements for the sea-based SNF under conditions of nuclear and conventional war have determined that their main combat use is patrolling the oceans and seas at considerable depths (hundreds of meters), which makes reliable communication with the SSBNs more difficult. The SSBN C^3 system allows SLBM launch both from submerged submarines and from the submarines on combat watch at their bases.

SSBNs patrolling submerged in peacetime are continuously on duty for VLF reception. Under combat conditions, the General Staff's order to launch missiles would be transmitted to the submarines by KSBU via the ground-based VLF transmitters and shore-based communication facilities. Once the launch order is received, the SSBNs should execute it without surfacing or conducting any two-way communications.

Communications between SSBNs and the center are possible only when the submarines surface. In this case, a session of two-way communication is conducted via HF and satellite channels. Submarines on combat duty in the oceans and seas surface in turns according to a special schedule, which is periodically changed. In an emergency, the center can use the VLF network to transmit a command to surface to one of the submarines, and then conduct a two-way communication session with it. Beginning in the early 1980s, urgent orders to surface have been transmitted by the ELF radio center *Zevs* (near the city of Severomorsk on the Kola peninsula), equipped with a transmitting antenna several dozen kilometers long.[151]

The Northern and Pacific fleets have shore communications facilities to support SSBN command and control. These facilities are connected via cable, satellite, radio relay, and radio channels with the command posts of the General Staff, of the main naval staff, and of the fleets, and also with the mentioned powerful VLF and ELF radio centers. If necessary, the Ministry of Communications' transmitters could be enlisted for SSBN command and control.

Russian SSBNs are equipped with safety devices blocking accidental or unauthorized launches of SLBMs. Their nuclear weapons can be unblocked only after a special code is received from the chain of command. From the very beginning, and until now, the crews of Soviet (Russian) SSBNs have not had a real ability to launch SLBMs without authorization by the chain of command.

The semi-automatic *Dalnost'* system has been installed at the main naval staff and fleet command posts, and at shore communication centers. This system increases the

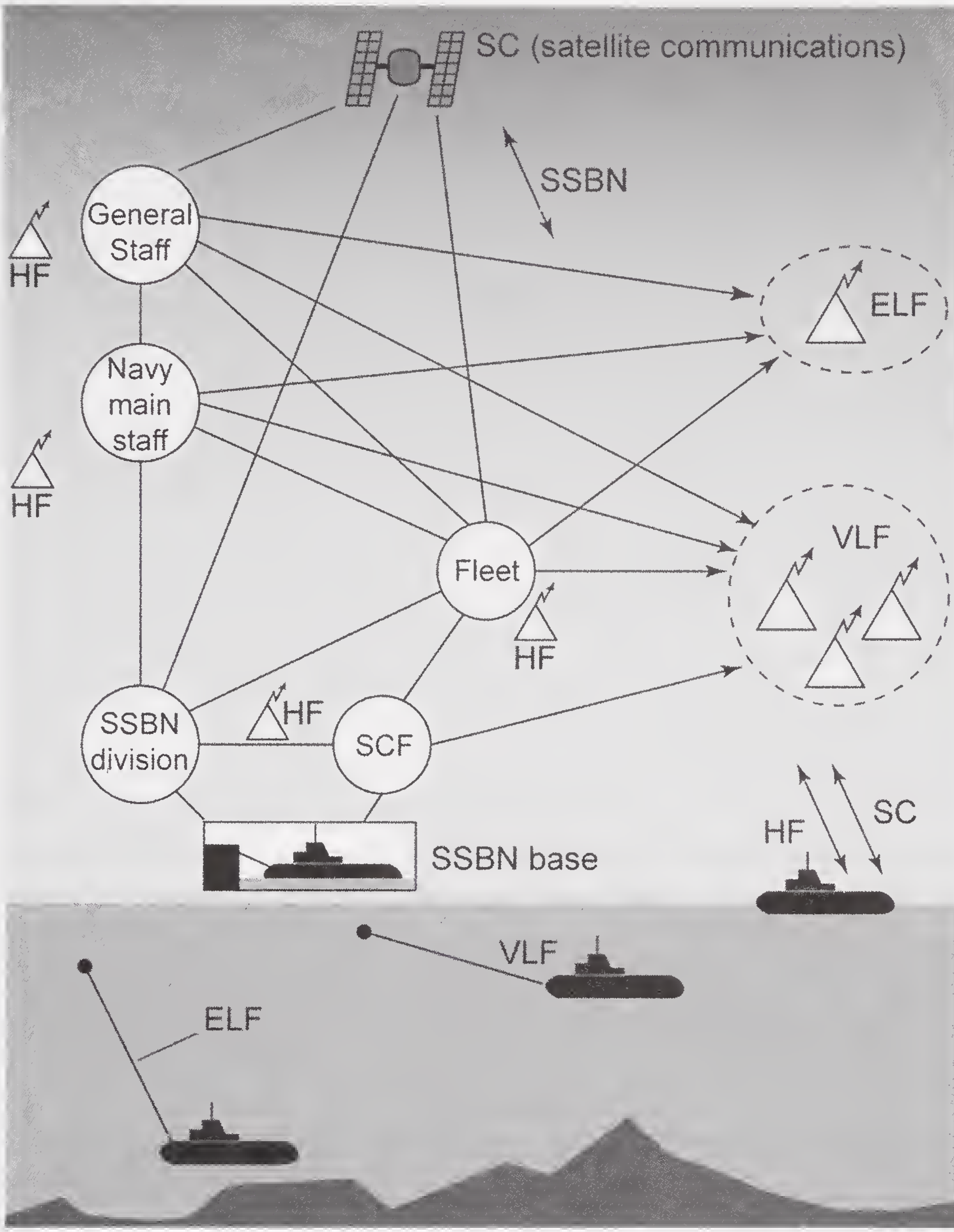


Fig. 40: SSBN C^3 system. (SCF – Shore Communication Facility.)

speed of relaying commands from the center to submarines several fold. The submarines themselves have been equipped with the *Rotator* and *Integral* (*bortovye kompleksy tekhnicheskikh sredstv*: on board technical devices), as well as devices for logic processing of incoming digital data from radio channels, and its delivery to the commanding officer and the weapons systems of the SSBN.

Work is being conducted to improve the reliability of transmitting orders by *Perimetr* to SSBNs under extreme conditions. It has been impossible to use *Perimetr* in its normal mode with the sea-based SNF because its working decimetric range radio waves

cannot penetrate deep water. *Perimetr*-type logic receivers are installed on SSBNs, but they receive orders from the command missiles by relay: initially, the orders are received by the ground-based elements of the sea-based SNF C³, and are then transmitted to submerged submarines by LF channels.

In the overall plan, a solution for this problem is foreseen within the framework of the mentioned *Tsentr* system, in which the planned subsystem *More* would serve the sea-based SNF.

The role of the Russian SNF's airborne component is currently reduced, and this study does not address its C³ system in detail. Fig. 42 shows several crucial details.

Communication with strategic bombers in flight is maintained via HF, VLF and satellite channels transmitted from ground bases. When the bombers are far away from their ground bases and under powerful jamming, transmitting the launch orders becomes quite complicated.

Command and control of that part of the airborne SNF which is located at airfields when the General Staff combat order is received, is more reliable. The crew, receiving all necessary data on the ground, i.e., the target destination and the code for unblocking the nuclear weapons, can in principle then take off, go to the target, and accomplish the mission independently.

Here a very serious "but" comes into play, although connected only indirectly with command and control: The most critical factor is to ensure that the airborne SNF take off from the ground before any surprise strike against them. The C³ system itself can rapidly deliver an urgent takeoff order to the airfields. But starting the engines and launching all the aircraft takes much more time. The bombers cannot start their patrolling beforehand and continue it for a long time, both because of technical limitations and because of strategic considerations. Such an action in a crisis situation could be provocative. All of this imposes certain limitations on the participation of the airborne SNF in a nuclear retaliatory strike.

In order to win several minutes and reduce losses to the airborne SNF, the following scenario was assessed during exercises in the 1970s and 1980s. A proposal was made to insert an order into the operational documents for urgent strategic bomber takeoff upon receiving the preliminary signal of an opponent's missile launch, even before the EWS comes up with a "missile attack" signal. But this proposed variant was recognized as unacceptable, since the takeoff of all forces upon an erroneous signal might provoke a strike against Russia.

Planned within the framework of the *Tsentr* project, the command and control system *Krylo* for the airborne SNF is now at the experimental design stage.

4.2.4 Scientists, Designers, Testing Ranges and Industry

From the very start until recently, the quality of Russian nuclear C³ and the speed of its development and introduction to the troops were largely determined by the powerful support rendered by the country's political leadership to the strengthening of the

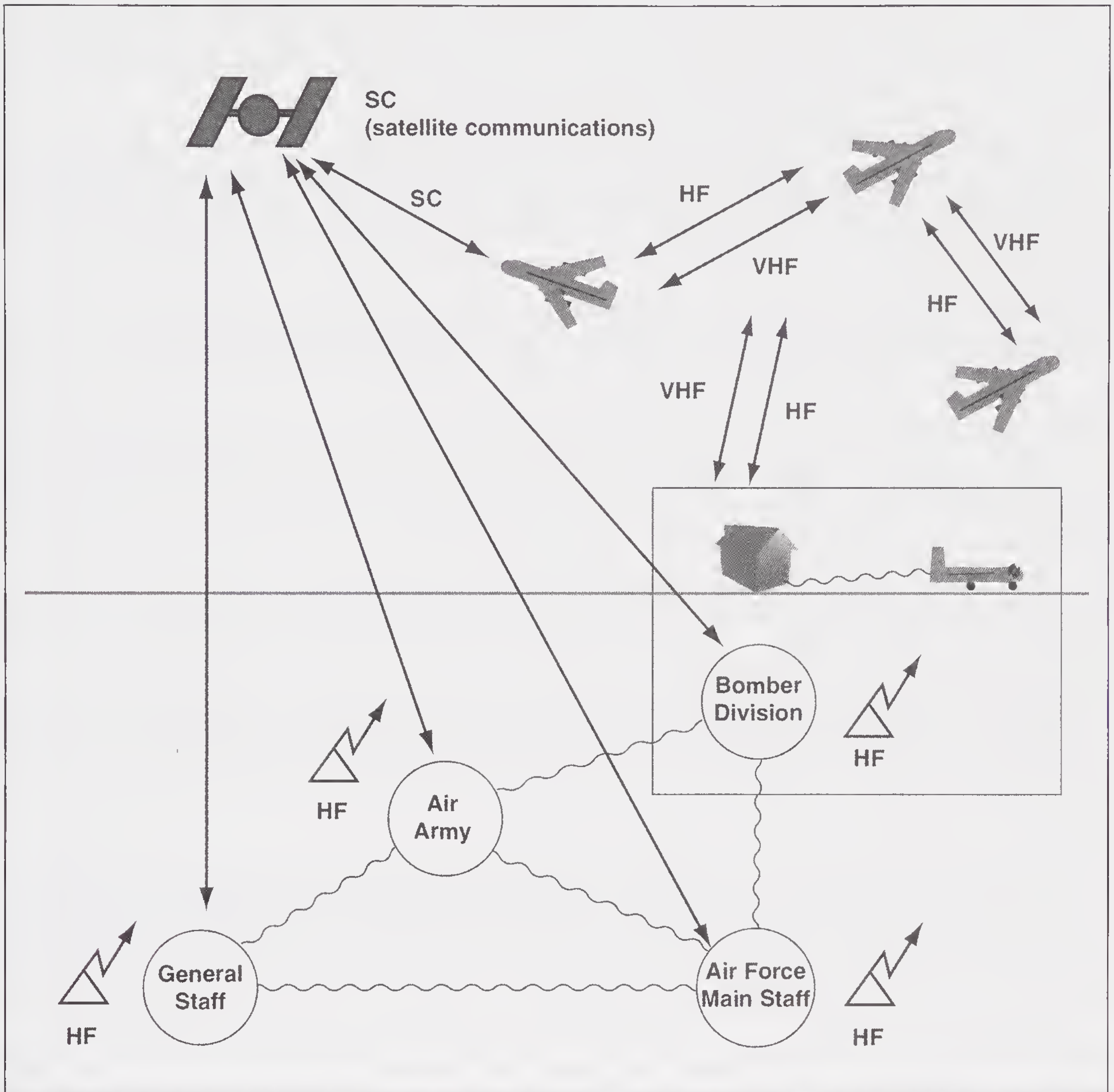


Fig. 41: C³ system of air component of SNF.

nuclear forces as a whole. The technical complexity of nuclear weapons and the unique nature of their use in combat demanded a close relationship between the military command structures and military/civilian research and development institutions, design bureaus, and industrial enterprises. This cooperation functioned not only at the tactical stage of technical development and testing, but also throughout subsequent use by the military.

Over the last several decades, each leg of the nuclear triad developed its own, relatively stable network of cooperation between research institutes, design bureaus and factories specializing in the development and modernization of C³ systems for strategic nuclear weapons. Table 6 shows the general principles of this cooperation.

The main doctrinal ideas for the development of C³ and the strengthening of its

combat potential are born in the central staffs of the various services, most prominently in the main staffs' operations directorates. These core ideas are directly formulated in the directorates' departments of troop control automation.

Subsequently, these initial requirements are forwarded to the military research institutions for detailed study. Each of the nuclear triad's military services has its own lead research institute, plus several other military research organizations (institutes, academies, centers and testing facilities) subordinate to it.[152]

The lead research institute in charge of all aspects of SRF development, including C^3, is the Central Research Institute No. 4 of the Ministry of Defense, located in the Moscow suburb of Bolshevo. Together with Institute No. 4, the Peter the Great Military Academy in Moscow, the Mozhaisky Military Academy in St. Petersburg, and a number of higher SRF officer schools do work on C^3, on a project-by-project basis. The Central Research Institute No. 30 of the Ministry of Defense in Moscow studies C^3 for the airborne SNF, while Central Research Institute No. 24 in St. Petersburg performs similar work for SSBNs. These research institutes of the nuclear triad cooperate with one another, as well as with Central Research Institute No. 27 in Moscow, the lead institute studying command and control for the Russian Armed Forces as a whole.

The military research institutes for each leg of the SNF triad analyze all aspects of new missions and develop the technical specifications for new technology, or for the modernization of an existing system. A draft of these requirements is presented to the customer – the main staff of the respective service.

After this, the main staff, together with the directorate of the service in charge of acquisitions, drafts an agreement with the manufacturer. The purpose of such an agreement is to ensure that the project can be indeed implemented according to the customer's specifications and within the estimated budget. Within the network of design organizations working for a given military service, the lead organization is the chief designer of the C^3 system for that leg of the nuclear triad. This group organizes a more detailed study of the given requirements, with the participation of all the civilian research institutes and design bureaus that are part of the network.

The lead organization for the SRF C^3 is the Impuls Corp. in St. Petersburg (director – B.G. Mikhailov, chief system designer – V. Ye. Petukhov). It cooperates on different aspects of C^3 with the Central Design Bureau of Heavy Machine-Building in Moscow; the Moscow Institute of Thermal Technology; the Moscow Research Institute of Radio Communications; the Voronezh Research Institute of Communications; the Krasnoyarsk Television Factory; the Krasnodar Instrument-Building Factory; etc.

After several iterative stages in negotiations, the service commander in chief and the chief designer approve the technical specifications. For a major project, the General Staff also approves the specifications.

New systems and equipment are developed and designed in design bureaus under military oversight by those research institutes that formulated the requirements. The customer also constantly monitors the process of design and development through its

Stages \ Cooperation elements	Main staff of service	Military Research Institutes	Main C^3 designer	Military overside in industry	Series factories	Testing Ranges	Troops
Main doctrinal ideas	+						
Project of technical specifications (TS)	+	+					
Agreement of TS	+	+	+	+			
Approval of TS	+		+				
Laboratory and factory tests		+	+	+	+		
Testing ranges		+	+	+	+	+	
Tests on military sites	+	+	+	+	+	+	+
Series production				+	+		
Introduction to military installations		+	+		+		+
Introduction to combat duty	+	+					+
Operation by troops and industry's oversight	+	+	+	+	+	+	+
Removal from use	+	+					+

Table 6: Russian C^3 Acquisition

permanent representatives to the design bureaus. These representatives constitute the so-called institution of military acceptance, common for the whole Russian Armed Forces. The main customer in Moscow will not accept any design-team project without the approval of the lead military representative.[153]

Experimental samples of the new command and control equipment developed by the design bureaus then undergo a series of tests: stand tests, interagency tests and military field tests, either of whole systems or their major components. State tests are conducted by the state commissions, which are comprised of the customer's representatives, research institutes, design bureaus, factories and military specialists. According to the results, the experimental samples are either launched into series production or returned to the designers for improvement.

Depending on the character and scale of tests, they may require various facilities:

laboratories, experimental production shops in design bureaus, factory stands, military installations or testing ranges. In the 1970s and 1980s, SRF C³ equipment was produced in the Russian, Belarussian, Armenian, Kazakh, Baltic and Ukrainian Union Republics. The major factories in Russia were the *Kalinin* machine-building factory and the *Bolshevik* factory in Leningrad, the *Barrikady* factory in Volgograd, and the factories in Krasnoyarsk and Krasnodar.

Since the disintegration of the Soviet Union, relations with the majority of C³ enterprises outside Russia have broken off or have become complicated, including such major enterprises as the Minsk Electrical-Mechanical Factory, the *Monolit* and *Kommunar* factories in Kharkiv, and the radio factory in Kiev. Certain steps have been taken to recreate the necessary network of factories within Russia itself.[154]

The new C³ systems and equipment are tested at the same scientific and testing center as the missiles themselves. The SRF usually use the well-known testing ranges Mirny, near the city of Arkhangel'sk, Kapustin Yar near Volgograd, and (now, to a lesser degree) Tyuratam in Kazakstan.

The special nature of nuclear C³ systems requires compulsory testing of their components with the respective ICBM systems. Tests of C³ systems are usually completed by live missile launches at the testing ranges or at military installations. If C³ tests are on a small scale, they are included as an element in the general program of testing new missiles. When large components of C³ systems are tested, missiles and other necessary equipment may be allocated for live launches at the final testing stage.

In this respect, the testing of *Perimetr* in the early 1980s was quite typical. A brief description of test procedure is useful. From the Impuls Corp.'s test stand (still the LPI Design Bureau in Leningrad at the time), which simulated the Central Command Post of the General Staff, a signal was transmitted by a regular communications channel to a LF transmitter near Moscow. Then, its signal was received at Kapustin Yar by the special mobile launcher of a command missile (based on the SS-20 *Pioner*). The command missile took off on a trajectory to Lake Balkhash (the impact site) and, for the entire duration of the flight, transmitted the launch order. This order was received in a silo launcher at the Tyuratam test range, playing, in this case, the role of a combat launcher. The ICBM also launched and precisely hit the target at a testing range in the vicinity of the Kliuchi settlement in Kamchatka. At the same time, many command and control posts – deployed for this test throughout the Soviet Union – received the order transmitted from the nose cone of the command missile.

As in the United States, the average term for developing Russian C³ components is about five to seven years. But in some cases, developing new equipment takes longer.

After testing, new C³ equipment is put into series production and introduced to military installations. As mentioned, at this point contacts between the military and the manufacturer continue. Moreover, one may say that this cooperation broadens because it includes a large number of military specialists from the troops.

The Russian SNF, especially the SRF, have developed regular cooperation with weap-

ons designers and manufacturers that lasts for the entire period in which equipment is being operated by the troops, until it is removed from use. This is the case for both the nuclear missiles and their C^3 systems. The arrangement described above has been called the "industry's guaranteed oversight." Essentially, the design bureaus and manufacturers are obligated for the duration of the equipment's life to conduct the difficult work at the military installations that the military cannot conduct. Among these are urgent repairs following accidents or major failures, takeover of equipment by the Ministry of Defense, prolonging service life, analysis of operation on a service-wide scale, etc. The Ministry of Defense annually allocates resources for the industry's guaranteed oversight.

Even today, factory teams, representatives of design bureaus and officers from military research institutes maintain a presence at the SRF installations. This approach has proven its effectiveness in general, and with C^3 in particular. As a rule, when the military requests them, the industry's specialists arrive at any military installation within one or two days and perform necessary repairs. Thanks to such rapid and skilled aid, the weapons and C^3 systems are maintained in a state of high combat readiness.

Western experts have shown consistent interest in the special character of decision-making and cooperation among those Russian military-industrial structures that are involved in the development and introduction of new weapon systems. It is worthwhile to comment upon certain ideas stated by Stan Woods, an American expert, in 1984 regarding Russian C^3.

Woods stresses the tendency of the Russian acquisition agencies to favor simple solutions, which allow effective implementation of the requirements without any "extras":

> "Soviet designs are often simple – meaning rugged, lacking detailed finishing, and tailored to a single role – and frequently they are able to perform the task required of them and no more. From the fact that many, but by no means all, systems fit this description, it cannot be inferred that they are any less effective, however. In fact, real operational benefits result from Soviet designers' preference for weapons containing a minimum of exotic materials or sophisticated subsystems and for employing the most advanced technology only if it is vital to successful performance of the combat mission."[155]

This conclusion is generally correct. The Russian C^3 system largely consists of such simple but effective modules, whose sum total provides for the required reliability of command and control. With few exceptions, all this equipment was developed and introduced into service on schedule. Today more than ever, Russia cannot afford any "exotic" technologies because of simultaneous drastic reductions in defense spending and sharp price increases for all parts and materials.

One can find similar conclusions about the tendency of Russian designers to stick to

an evolutionary development of military technology: "As for evolutionary change (or exploitation of design inheritance), there is an apparent Soviet preference for cautious step-by-step modification of hardware rather than radical design innovation."[156]

There are quite a few such examples in the Russian C^3 acquisition process, an example being the history of gradual modernization for the SRF C^3's main system *Signal*, described in section 4.1.

Woods notes with approval the practice of speedy introduction of new systems into service: "The Soviets attempt to deploy new systems as quickly as possible ... The Soviet practice of prototyping enables a weapon in every case – to reach operational status very quickly."[157]

This is generally true, although when it comes to C^3 equipment there is a difference. The approach described above cannot be applied to the process that the designers and manufacturers use to perfect the reliability of negative control in new types of C^3 systems. Until all the requirements for protection against unauthorized actions are fulfilled and confirmed during tests, prototypes are not launched into series production. As for any new operational capabilities in C^3 technology, sometimes permission can be obtained to improve them to the level already being introduced into service, or even during the early stage of combat service. This would be within the framework of the industry's guaranteed oversight, as described earlier. This principle is applied also to the introduction of the newest missile systems, which include as integral parts C^3 elements at the lowest level.

Woods' study also criticizes the belief that Russian design bureaus completely depend upon research institutes, a mass of reference manuals, instructions and various requirements, which are said to practically paralyze the initiative of the new weapon designers:

> "The relationship between research institutes and design bureaus profoundly influences the Soviet [research and development] process ... Their [different restrictions'] existence is a reflection of the institutes' monopoly of research and test facilities. It is said that this style of [research and development] inhibits designers from exploiting new technologies that could lead to important weapons development. But to argue this is to ignore the military effectiveness of many Soviet weapons and rely on assertions about their low technological content."[158]

Obviously, there are some formal restrictions on what the designers can do, but it is erroneous to say the designers are completely helpless in the face of the customers. As noted earlier, the Russian C^3 designers play a role equal to, and sometimes even more important than, that of the military in the research and development process. A good example of this can be found the history of the Impuls Corp., published in Russian in 1995. There, in a memoir about Taras Sokolov, the general designer of the SRF C^3 system, V. I. Lazutkin, one of his closest aides and a winner of Lenin and State prizes, writes:

> "[Taras Sokolov] used to say that the customer's technical requirements for the development of complex systems is not the Koran, but only a movie script. The resulting movie depends on those making it – the director, the actors, the cameramen, the composers. It depends upon how deeply they understand their mission, how unified their team is, and of course, upon the customer himself. As a result, the quality and success of the movie are determined by the talent and mutual understanding of its creators; and, most importantly, the most successful movie is not the one that the customer initially wanted, but the one that he really needs."[159]

The military customers in Russia, just like their Soviet predecessors, have not objected to such a cooperative approach as a rule, and have largely trusted the innovative views of highly-qualified civilian specialists regarding the complicated problems of nuclear command and control. Still, there have been many arguments. If there are any restrictions on new developments, especially now, they are the result of insufficient funding, as already mentioned.

In his conclusion, Woods, comparing the practices of weapons acquisition in Russia and the United States, considers the Russian approach – simpler, but less expensive and more reliable – quite sensible:

> "This is why Soviet weapons are often simple in comparison with overly sophisticated U.S. equipment. And it is why Soviet hardware is notoriously poorly finished by Western standards. In the trade-off between production costs and high weapon capability, Soviet designers tend toward the former when possible. Low production costs permit the procurement of large numbers of sturdy, reliable, and militarily effective systems. On the other hand, the quest for high weapon capability can result in extremely expensive, unreliable equipment, which may perform poorly in battle."[160]

Naturally, one should not idealize "simplicity." Technical progress is inevitable and should not be artificially slowed down, including the area of new weapons development. However, in such a special area as nuclear C^3, simplicity and reliability, perhaps, should be the guiding principles. Apparently, the Russians stick to these principles.[161]

Russia owes its C^3 system to many talented and outstanding individuals, both military and civilian. In section 4.1, I already named the General Staff's generals who determined the doctrine and shape of the highest level SNF C^3, and, together with specialists from the Navy and Air Force, the direction of C^3 development for the sea-based and airborne legs of the triad. As for the command and control of land-based missiles, the most prominent roles have been played by the following SRF customers: Gens. Alexander Sapozhnikov, Ivan Dyukarev, Dmitry Gal'tsov, Varfolomey Korobushin, Igor Sergeev, Yuri Yashin, Victor Esin, Alexander Ryazhskikh, Igor Kovalev, Victor Khalin,

Victor Petrankov, Yuri Pikin, Eugeny Volkov, Lev Volkov, Vladimir Dvorkin, Victor Dolgov, Anatoli Kulibaba, Mikhail Pokushko, Valery Rudakov, Valery Subbotin; Cols. Yuri Mosalov, Boris Uchenik, Grigory Ioffe, Yuri Kasatkin, Pavel Zolotarev, Alexei Nefedov, Vladimir Kolganov, Yuri Ksenofontov, Vitaly Zhikin, Alexander Larin and Boris Fedotov, and many other generals, officers and civilian specialists of the SRF.

In addition to the chief industrial designers and experts named in section 4.1, who played a prominent role in the development of SNF C^3, one should mention Anatoli Aleksandrov, Stanislav Sametskiy, Eugeny Kamushkin, Gennady Valentik, Vadim Kondrashov, Vitaly Teterev (all from the Impuls Corp.), Anton Bilenko, (Moscow Institute of Radio Communications), Boris Osipov and Vladimir Borisov (Voronezh Research Institute of Communications), Valery Romanovskiy (Moscow Institute of Thermal Technology), Boris Aksyutin, Alexander Leontenkov, Gleb Vasil'ev (Moscow Central Design Bureau of Heavy Machine Building), Leonid Pokrovskiy (Krasnoyarsk Television Factory), Yuriy Khoroshkin (Krasnodar Instrument-Building Factory) and Yuri Zagorovskiy (the *Monolit* factory in Kharkiv); among others.

Despite the natural differences of character and career between these military and civilian specialists, they have always been united by enthusiasm for and lifelong attachment to their work. Probably, the majority of them – being highly-educated, intellectual people – never seriously believed in the acceptability of nuclear war, and did not consider the danger of aggressive "world imperialism" to be the main stimulus of their activity. Also, the modest salary paid in the Soviet Union, and now in Russia, to the chief designers of the mighty C^3 systems and their associates was not their motivation. Many of them have advanced degrees, are professors and members of the Academy of Sciences, and winners of state prizes and other awards.

Most probably, when thinking through and implementing new ideas for nuclear command and control, these people have been motivated by purely professional interest in such an esoteric field, as exciting as space exploration. Indeed, in many cases, components of military C^3 systems are used for space programs, while the research and development and industrial organizations involved with C^3 also receive direct orders for specialized, non-military systems and equipment for space exploration programs. The majority of enterprises involved in C^3 also have substantial achievements in other cutting-edge areas of Russian science and technology.

A good example is the Impuls Corp., which, since 1995, has been openly described as Russia's lead design organization for SRF C^3. Established in 1961 at one of the leading science and technology centers in Russia (the LPI, now the St. Petersburg State Polytechnic University), Impuls Corp. has to its credit, in addition to its main work, the development of one of the first Soviet digital computers (*Kvarts, Temp-1, Temp-3*); participation in launches of the first earth satellites and the first manned space flights, beginning with Yury Gagarin's pioneering flight; contributions to the theory and practice of magnetic microelectronics; dynamics of nuclear power stations; automation of experiments in ballistics; computational technology; and medicine. Beginning in the

1990s, as part of a defense industry conversion, Impuls Corp. has been designing and producing modems, information security equipment, information utility networks, multifunctional credit payment systems and RAMEC/IMI computers. The Impuls Corp. is cooperating with a number of U.S., German, French, Japanese and other companies. So far, of course, this cooperation does not include issues of command and control.

Other Russian enterprises involved with the development and manufacturing of nuclear C^3 systems also have sufficiently broad interests and connections.

In this network of people involved in interesting practical matters, officers from the military research institutes play an important role. They are not abstract theorists but rather practical specialists, as knowledgeable in the details of new C^3 systems as the designers themselves. For instance, the officers at the Ministry of Defense's Central Research Institute No. 4 are regularly included in the commission for testing new missiles and their C^3 systems. They spend months at a time working together with industry representatives at testing ranges and military installations.

The development and testing process for C^3 system components is quite interesting. Initially, a rational and concrete idea is formulated during several, sometimes very difficult, discussions between the customer and the contractor in Moscow and St. Petersburg. Then this idea is tested by representatives from both sides in some picturesque place, such as the steppe of Kapustin Yar, or the Siberian taiga. There, these recent intellectual opponents live and work together as a family, despite a frequent lack of creature comforts. These people know not only how to work, but how to have a good time too: hunting, fishing and conversations around a campfire at night. And finally, their common hard work is crowned at the testing range with the fantastic, unforgettable sight of an ICBM launched by a "button" they have designed. Among congratulations and compliments, no one even remembers the "potential aggressor." And again, the next day will see fierce arguments about ideas for new work.

Unfortunately, this style of work is more characteristic of the recent past. Today, things are different. Changes in Russian mentality, the limitations in defense spending and a number of other factors have negatively affected the cohesion and effectiveness of the C^3 research, development and production network. In order to pay their employees on a regular basis, and somehow preserve their companies' intellectual potential, the leaders of the design bureaus and research institutes have to look for contracts unrelated to their real expertise. Despite these efforts, however, there is a serious brain drain from the Russian C^3 community. Many young, capable people leave these organizations for better-paying jobs, frequently in trade.

There were even strikes at enterprises producing strategic C^3 equipment. In February 1997, workers and engineers of the Impuls Corp. in St. Petersburg took to the street, demanding that they be paid salary owed them for eight months. This incident, unthinkable only several years earlier, received attention from mass media not only in Russia but also in the West, a publicity that helped solve the problem rather quickly. Under Putin, there has been no information about similar incidents.

The negative impact of such developments is evident. As noted in previous chapters, a strong C^3 system in any country is a stabilizing factor. A weak C^3 system is a provocative one. Russia's present problems will make everybody a loser.

The history of the Impuls Corp., cited earlier, says:

> "Lucky are those who spent their young years participating in great deeds for the glory of the Fatherland. This can certainly be said about us, the authors of this book ... Working at the cutting edge of space science, we established unique creative teams. Among us were the generators of ideas, the top-notch specialists on research methods, the unique system analysts, the irreplaceable 'directors' who staged scientific experiments, and those with the special gift for introducing new technology into production and service – nothing would have been achieved without all of them. ... We worked without respite, without fatigue, without fear, finding strength in our optimism and confident knowledge that we were a part of a grandiose project, one of the most prestigious and exciting ever. ... Our ambition – both personal and patriotic – found its manifestation in voluntary cooperation, when each one of us felt his direct contribution to the common cause. We were young, daring and inquisitive then. We all wanted to accomplish something new, unforgettable. And we were really lucky ..."[162]

Well said. We should think about ways to preserve these excellent traditions, great experience and high professionalism in order to provide and strengthen strategic stability.

4.2.5 Prospects for Development

Changes in the international situation, the tempo of strategic arms reductions, scientific and technological progress, and the economic and political situation in Russia influence the development of the Russian nuclear command and control system. Changes in the Russian SNF C^3 system will be determined, first of all, by any structural and qualitative changes that may take place in these very forces.

The first decade after the end of the Cold War and the disintegration of the Soviet Union was generally characterized by improvement of U.S.-Russian relations and by progress in reductions of the two nations' strategic nuclear arms. In Russia, this process was primarily determined by the economic conditions: the missiles and their infrastructure, produced in the 1970s and 1980s, were past their service life, and, despite all the effort to extend it, were gradually removed from combat duty and decommissioned, that is – destroyed. Russia could no longer maintain the old arsenal of 6,000 to 6,500 nuclear strategic warheads.

The logical result was a revision of outdated concepts of deterrence and a move away from the old, mistaken assessment methods of its reliability and sufficiency. One should pay respect to Putin: after some vacillation, he has demonstrated an understanding of

the reality and moved against the calculation and forecasts of official military experts. A primitive approach based on numerical parity of missiles and warheads, as well as the erroneous method relying on average magnitudes of retaliatory strikes, turned out to be useless when the Bush administration took the course toward national missile defense (NMD). It has become clear that the old approaches to nuclear deterrence reel only into a dead end, at least because standard instruments are of no use for analyzing such a unique phenomenon as global nuclear catastrophe. And the Russian president, who initially responded with threats of MIRVing SS-27 Topol-M ICBMs in response to NMD, has quickly found his way around the issues of strategic nuclear policy, and has offered a reasonable deal. In exchange for allowing U.S. work on NMD, Russia has obtained a U.S. pledge to cut deeply its offensive strategic arsenal, as well as other political dividends. Russia's choice in the sphere of nuclear weapons has become especially important since it has been undertaken within the context of another crucial decision by Putin, the one to support the United States in its fight against international terrorism, which can become dangerous to Russian nuclear-tipped missiles and their C^3 system.

While the process of Russian nuclear arms reduction in the last 10 to 12 years has followed the path of logic, the structural changes of the SNF and military reform as a whole hardly followed the same road. Two ministers of defense, Gen. Pavel Grachev (1992-1996), and Gen. Igor Rodionov (1996-1997) widely advertised their plans for military reform, but nothing has been accomplished during their terms on office. To be more precise, a spontaneous "military reform" amounted to disintegration of the Armed Forces. The SNF also experienced difficulties, but continued to be the backbone of the Armed Forces, the main means of deterrence.

The first real steps toward reforming the SNF were made in 1997-1998, when Marshal Igor Sergeyev, the minister of defense, merged the SRF with the space troops and BMD troops. This was the beginning of a serious plan for the integration of SNF command and control. Next, plans were announced for the creation of a joint command of Russia's SNF, along the lines of U.S. Strategic Command (STRATCOM). But Russia's financial collapse in August 1998, as well as the unprecedented open conflict between the chief of the General Staff, Army Gen. Anatoly Kvashnin, and Sergeyev, which ended with the latter's resignation, resulted in a drastic change in the Russian leadership's approach to SNF reform in 2001. The space troops and BMD troops were removed from the SRF command and subordinated directly to the General Staff. The SRF have lost their status as the most important service of the Armed Forces, and are supposed to be subordinated to the Air Force by 2005-2006. The SNF have started to emphasize SSBNs, while the emphasis in the Armed Forces as a whole has shifted from nuclear weapons to conventional ones.

These unpredictable zigzags in the process of SNF reform could not but have an impact on their C^3 system. During these years of uncertainty there has been no real plan for development of the Russian strategic C^3 system. Furthermore, the situation

has been complicated by meager funding of the defense budget, and a fundamental restructuring of the defense industry begun in 2001. At the same time, throughout this whole period the Russian military and political leadership have understood, or at least have declared that they understand, the role of C³ in robust nuclear deterrence. Many statements have been made to the effect that further nuclear arms reductions should be accompanied by strengthening the C³ system. For instance, Sergeyev, while still SRF's commander in chief, said in 1995: "The command and control system has always played a special role in ensuring combat readiness of the SRF. Today, when SNF undergo significant reductions, the important of command and control is growing, since the quantity of weapons is going down, and their guaranteed employment requires absolutely reliable and survivable C³ systems."[163]

The former chief of the Main Operations Directorate of the General Staff, Col. Gen. V.M. Baryn'kin wrote: "One should emphasize that when troops (forces) are being reduced, their effective employments becomes one of the main tasks, and their command and control system become the main factors providing for deterrence."[164]

Today, all information regarding the directions of the SNF C³ modernization is classified, and therefore one can make only some conjectures derived from the general character of Armed Forces reform.

Although Sergeyev's plan for a joint strategic command has been abandoned for now, the integration of SNF C³ will not fade away, and the issue requires a solution for a number of complex organizational and technical problems. This is a result of increased general requirements to modernize C³ systems, as well as of the ongoing structural changes in the Armed Forces. First, turning space troops into a separate branch subordinated to the General Staff presumes improved coordination of satellite communications channels, navigation data and EWS information, providing support to all the components of the nuclear triad, as well as to the conventional forces. Second, the planned inclusion of SRF into the Air Force as a service branch will require a substantial reorganization of the command posts and lines of communication, and a change of combat planning documents in cooperation of different formations for accomplishing a joint SNF mission. With the Main Command of the Ground Forces restored, there must be new tasks to organize command and control of tactical nuclear weapons, and to coordinate their C³ with the common principles of command and control of nuclear weapons as a whole. Finally, the growing threat of international terrorism requires a more energetic effort to strengthen the reliability of negative control over C³ in all formations armed with nuclear weapons. Today, all such problems are the prerogative of the General Staff. Will it be able to resolve all of them as their number and importance continue to grow? Perhaps it will be necessary to create a special body responsible for a complete solution.

In addition to integration, Russia's strategic C³ development will include:

- The deep SRF reductions, and the character of recent agreements regarding strategic arms reductions, will cause intensified work on increasing the reliability of

command and control of SSBNs and land-based mobile ICBMs.

- In order to provide for reliable deterrence within the LUA framework and with this concept becoming the main one, survivability of the system of central command posts is likely to continue to be strengthened. This can be achieved by developing its mobile (ground and airborne) elements, as well as by improving the stationary command posts.
- The existing multiplicity of types of C^3 systems in the various SNF elements is recognized to be a serious shortcoming. The experience and available designs of the research, development and production enterprises working for SRF, which involve some technological solutions applicable to SNF C^3 as a whole, can help solve this problem.
- Information transmission priority will apparently see development of special radio channels for combat command and control, satellite communication systems, methods of digital information processing, use of communication lines of other agencies and state-owned civilian networks for the needs of SNF.
- Maximum use of computers will continue to be one of the main requirements for improvement of SNF C^3.

If the assessment of the reliability of nuclear deterrence, one that incorporates proper attention to the C^3 factor, became an official one, it would allow to clearly determine the most rational structure and characteristics of C^3 for nuclear forces. Such an optimal system must be appropriate for LUA and have the following characteristics:

- A group of central command posts that ensure with sufficient probability that an order to launch a retaliatory strike will be issued after an enemy attack has already made its impact. The required systemic survivability of the central command post group can be achieved by using mobile command modules, super-hardened stationary facilities or an optimal combination of both. If such a system of high-level command posts existed in a crisis, it would permit the decision to use nuclear weapons to be made without dangerous haste. Absence of such an element in the C^3 system is a destabilizing factor.
- A system of direct communications channels, as survivable as the central command post group, linking these command posts with nuclear weapons delivery systems. Clearly, it is necessary to have such reliable communications with the means of retaliation (in Russia, these are SSBNs and mobile SS-25 ICBMs *Topol*). The main requirement for these channels is the ability to function despite the impact of nuclear and high-precision conventional weapons, electronic jamming and EMP. At the same time, the speed of the launch order transmission is not crucial.
- An accurate global system for identifying a nuclear or massive conventional attack, with sensors distributed all over the nation's territory, and with channels for transmitting information from those sensors to the central command post group.

Such a system would provide for a more accurate estimate of current damage to the friendly side, to be used in a subsequent determination of what constitutes a threshold level of damage after which it becomes possible to use nuclear weapons in the course of a conventional war. Naturally, the determination of this threshold in the course of war is very difficult. Still, it would be better to understand the complex situation before deciding to use the means of last resort – massive employment of nuclear weapons.

- A reliable subsystem of command and control for the forces and means used to guard and defend nuclear weapons delivery systems (for instance, surface ships in the areas of SSBN patrols).

Worldwide safety of nuclear weapons can be enhanced by external control over its C³ system. It would make sense to link the five nuclear powers' national C³ systems together into a unified automated system of control and cooperation. Such a system must give all participants the capability for continuous mutual control over readiness and technical condition of nuclear weapons, record any attempts to penetrate command and control systems, and prevent unsanctioned and accidental launches of missiles. At the same time, the unified automated system of control and cooperation should not limit freedom of action regarding the use of those weapons. Such a system is technically feasible, but appropriate political decisions for its implementation are missing.

Obviously, international cooperation would allow us to determine the most rational character of nuclear command and control systems and develop a standard for them. This would make it much easier to formulate requirements to each system, and would prevent excessive spending.

Naturally, it will be difficult to achieve all these goals. This section addresses only some possible positive prospects for the development of the nuclear command and control system, and so far it is difficult to say how Russia will resolve these problems. Until now, neither Russia nor the United States nor the other nuclear powers has raised the issue of common C³ standards. But today this issue is urgent in light of these systems' exceptional importance in ensuring strategic stability.

4.3 C³ in the United States

Various questions concerning the U.S. nuclear command and control system are discussed in Chapters 2 and 5 of this book. Chapter 2 presents the opinions of American authors on the general evaluation of the system developed in the 1970s and 1980s, and Chapter 5 analyzes a comparison with the Russian C³ of specific problems like the reliability of negative control, the survival capabilities of the system under battle conditions, and questions of delegating authority.

This section seeks to provide a picture of the American C³ in the late 20th-early 21st century and impart some additional information.

It is pointless to attempt to describe here all of the open-source information on the

U.S. nuclear command and control system: first of all, because of the large volume and continuous updating, and secondly because it is quite difficult to isolate this system from the background of the extensive national military and civilian networks of administration and communication that are well-integrated at various levels. The objectives here are somewhat different: To show how openly Americans discuss their C^3 and to help the general reader to find information that is of interest to him or her on this topic on the Internet and in various publications. At the same time, even separate fragments of the system provide a relatively thorough understanding about its extensiveness, flexibility and security, the history of its development, its cost and its perspectives. It is possible that coverage of such information on the U.S. C^3 will allow the continuing secrecy of this sphere in Russia to be surmounted faster.

4.3.1 Command Posts and Centers

4.3.1.1 – Succession of command

A line of succession for command of the nuclear forces and of the country as a whole in emergencies has been developed and officially approved. The U.S. president's 12 successors in order of preemption are: the vice president, the speaker of the House of Representatives, the president pro tem of the Senate, and nine members of the Cabinet. This list is published in the Federal Register. Most departments and agencies have also determined and published lines of succession.

(http://www.fas.org/nuke/guide/usa/C3i/cog.htm)

4.3.1.2 – Supreme command

The supreme organ of command of the U.S. Armed Forces (including the strategic nuclear forces) is the National Command Authority (NCA), which includes the president and the secretary of defense, and their alternates and successors from the White House, the Pentagon, Congress, the State Department and other official administrations, the duties and rights of which are established in advance. Below the East Wing of the White House lies the President's Emergency Operations Center (PEOC), which exists to handle nuclear contingencies. The PEOC is differentiated from the White House Situation Room, which is located in the basement of the West Wing of the White House.

(http://www.fas.org/nuke/guide/usa/C3i/peoc.htm)

4.3.1.3 – Nuclear "football"

The president's nuclear briefcase - nicknamed the "Football" – contains nuclear launch codes (Gold Codes) and the President's Decision Book. The military officer who follows the president wherever he goes, carrying the Football, must be knowledgeable about all aspects of the overall Single Integrated Operational Plan (SIOP), as

well as the various options available to the president for implementing the war plan. The officer comes from one of the four military branches – ranked lieutenant colonel, naval commander, or marine major – and must undergo the nation's most rigorous security background check, "Yankee White." The criteria for this clearance include U.S. citizenship, unquestionable loyalty, and an absolute absence of any foreign influence over the individual, his family, or "persons to whom the individual is closely linked."

According to 2000 data, the SIOP involves four strategic targeting groups: Russian Nuclear Forces, Conventional Military Forces, Military and Political Leadership, Economic and Industrial targets. The "Black Book" contains 75 pages of scenarios for action: options of general attacks as well as selected or limited strikes. Nuclear forces can also be used against enemy forces leading a conventional attack against the U.S. or its allies.

The National Security Agency (NSA) has jurisdiction over all questions concerning the Football. It is also in charge of distributing the daily Gold Codes to the White House, Pentagon, STRATCOM and the TACAMO aircraft.

(http://www.fas.org/nuke/guide/usa/C3i/nuclear-football.htm)

4.3.1.4 – National Military Command Center

The National Military Command Center (NMCC) is located in the Joint Chiefs of Staff (JCS) area of the Pentagon. The NMCC is responsible for providing the JCS with information about the current state of the strategic forces as well as missile warnings. About 300 people are employed at NMCC. It is funded by the Air Force. The Center has the following facilities: the Current Actions Center (CAC), the Emergency Conference Room (ECR), and the JCS Conference Room, or "The Tank."

(http://www.fas.org/nuke/guide/usa/C3i/nmcc.htm)

4.3.1.5 – STRATCOM

The U.S. Strategic Command (USSTRATCOM), located on Offutt Air Force Base, in Omaha, Neb., is directly responsible for command of the nuclear triad.

The USSTRATCOM Command Center is located in the Underground Command Complex. Also located within this complex are the Intelligence Operations Center, the Weather Support Center, and the Alternate Processing and Correlation Center (APCC). The APCC conveys missile warning information from the Cheyenne Mountain Air Station (CMAS) for U.S. Space Command (USSPACECOM) complex in Colorado Springs, Co.

The USSTRATCOM Command Center is a two-level, high-altitude electromagnetic pulse (HEMP) protected facility that lies at a depth of 15 meters and has an area of about 1,500 square meters.

The main room of the Command Center has monitoring screens with a total length of about 80 meters. One thousand people work at the Control Center, and 800 of them

can remain there for two weeks under a fully autonomous regime. The Primary Alerting System, also known as the "Red Phone" system, enables USSTRATCOM controllers to speak directly to approximately 200 operating locations throughout the world, including intercontinental ballistic missile (ICBM) launch control centers (LCCs). There are direct lines to the president, the Joint Chiefs of Staff, and the National Military Command Center in Washington, D.C.

The Command Center is equipped with all channels of communication, including cable, very low frequency (VLF), low frequency (LF), ultra-high frequency (UHF), and high frequency (HF).

(http://www.fas.org/nuke/guide/usa/C3i/cmdctr.htm)
(http://www.stratcom.mil/factssheets/cmdctr.html)

4.3.1.6 – The Cheyenne Mountain Complex

The Cheyenne Mountain Complex (CMC), located outside Colorado Springs, Co., is the main correlation center of the Integrated Tactical Warning and Attack Assessment (ITW/AA) system. The CMC coordinates and controls the North American Aerospace Defense Command (NORAD) and the United States Space Command (USSPACECOM) missions. The primary functions of the object can be described with the words "missile – atmosphere – space" warning activities.

The Cheyenne Mountain Complex houses the following operation centers:

- The Air Operations Center (AOC) maintains constant surveillance of North American airspace to prevent overflight by hostile aircraft. It tracks over 2.5 million aircraft annually;
- The Missile Warning Center (MWC) detects launches globally and determines whether they are a threat to North America;
- The Space Control Center (SCC) detects, identifies and tracks all man-made objects in space. It currently tracks over 8,000 objects including payloads, rocket bodies and debris;
- The NORAD/USSPACECOM Combined Command Center (CCC) serves as the hub for all activity within the work centers. It forwards critical information from the other centers to the president of the United States and the prime minister of Canada. The center also reports to the National Command Authorities (NCA), the USSTRATCOM and other organs;
- The Combined Intelligence Watch Center (CWIC) serves as the indications and warning center for worldwide threats from space, missile, and strategic air activity, as well as geopolitical unrest that could affect North America and U.S. forces/interests abroad;
- The National Warning Facility is the U.S. civil defense warning center. In case of attack, the center would sound the alarm over the civilian alerting circuits of the

National Warning System (NAWAS);

- The Space and Warning Systems Center (SWSC) is responsible for the maintenance and evolution of mission-critical software. The SWSC currently maintains in excess of 12 million lines of code on 34 separate operational systems written in 27 languages;
- The Weather Support Center.

Five crews man the centers. Each crew consists of approximately 40 people, and, under normal conditions, each crew is on duty for an eight-hour shift.

An Alternate Missile Warning Center is located at Offutt Air Force Base in Nebraska.

Five upgrade programs planned for the Cheyenne Mountain Complex in 1987 were estimated to cost $968 million. In practice, however, the modernization took eight years longer than expected, and ran $792 million over budget.

(http://www.fas.org/nuke/guide/usa/C3i/cmñ.htm)

4.3.1.7 – Mobile Consolidated Command Centers

Two commands, the U.S. Strategic Command (USSTRATCOM) and the U.S. Space Command (USSPACECOM), have a joint mobile consolidated command center, called the Cheyenne Mountain and CINC Mobile Alternate Headquarters (CMAH), or Mobile Consolidated Command Center (MCCC).

The mobile center is mounted on special semi-trailers. There are several types of modules (trailers) that correspond to their functions: war planning, intelligence, communications, support systems (fuel, water, recreation, etc.). Several mobile command centers are configured from these modules.

An RF cable distribution system provides the internal communications. Communications systems, including HF and VHF/UHF radio and satellite (AFSATCOM, and MILSTAR) terminals, provide continuity of command capabilities. The communication terminals have electromagnetic pulse protection.

The U.S. Air Force is responsible for support of these command centers.

The United States has a network of airborne control centers at various levels of command. Two of them deserve special attention.

(http://www.fas.org/nuke/guide/usa/C3i/cmah.htm)

4.3.1.8 – National Airborne Operations Center (E-4B NAOC)

The E-4B National Airborne Operations Center serves as the airborne control center at the highest command level (the NCA and the JCS). There are four E-4B aircraft and they are based at the Offutt AFB in Nebraska. The NAOC is also the worldwide, survivable, enduring node of the National Military Command System (NMCS).

The E-4B is designed on the basis of the commercial Boeing 747-200, and has three

times more functional space than the earlier EC-135 command post. The main deck is divided into six functional areas: a National Command Authorities' work area, a conference room, a briefing room, an operations team work area, and communications and rest areas.

The E-4B crew may include up to 114 people. Its communication systems and terminals have electromagnetic pulse protection. The total weight of the EB-4 is 360 tons, its ceiling is 9 kilometers, its endurance is 12 hours unrefueled, and its cost is $258 million.

At least one E-4B is always on alert at one of many selected bases throughout the world.

The first B model was delivered to the Air Force in January 1980, and, by 1985, all four aircraft were converted to B models.

(http://www.fas.org/nuke/guide/usa/C3i/e-4bnaoc.htm)

4.3.1.9 – Airborne STRATCOM Command Center (E-6B)

The special EC-135 aircraft (nicknamed "Looking Glass" because its mission mirrored ground-based command, control, and communications) served as the airborne STRATCOM command center from Feb. 3, 1961 until Oct. 1, 1998. There were several such aircraft, and one of them was always in the air throughout all of this time. The crews accumulated more than 281,000 accident-free flying hours. On July 24, 1990, Looking Glass ceased continuous airborne alert, but remained on ground or airborne alert 24 hours a day.

The EC-135s have been replaced with the E-6 aircraft. An innovative decision was made to combine in one aircraft both Airborne Command Post (ABNCP) and Take Charge and Move Out (TACAMO) functions. The E-6A TACAMO aircraft was modified to a dual-mission aircraft, the E-6B. The USSTRATCOM is thus able to use all 16 dual-mission aircraft, with two aircraft at its disposal on alert status at Offut AFB.

The main modification for STRATCOM has been the installation of the Airborne Launch Control Center (ALCC), which is capable of determining missile status in silos, changing missile assignments, and, if necessary, launching missiles. The ALCC operates through the UHF range within the line of sight of the launch silo. The ALCC terminal is installed into a specially designated place as the given E-6B aircraft is equipped especially for STRATCOM once at Offut AFB.

The airborne command center relays orders to submerged submarines through the TACAMO system that comes standard in the aircraft model. For additional tasks, the E-6B is equipped with three 1,000-watt UHF radio stations, which have 45 full-duplex channels each, SATCOM (satellite communications) and MILSTAR (Military, Strategic, Tactical And Relay) terminals and other means of communication.

(http://www.fas.org/nuke/guide/usa/C3i/ec-135.htm)
(http://www.fas.org/nuke/guide/usa/C3i/e-6b.htm)

4.3.1.10 – ICBM Launch Control Center (LCC)

The website cited below describes the importance of the control system: "Survivable communications are an integral part of U.S. deterrence strategy because potential adversaries must be convinced that launch orders could actually be transmitted to, and received by, the Launch Control Centers (LCC) when required."

There are 100 LCCs for Minuteman and MX missiles, interconnected within each ICBM wing by an underground communication cable network. Each LCC controls and maintains in permanent readiness a flight of 10 silo-based ICBMs. At the squadron level (50 silos) any two LCCs working together are capable of launching all 50 missiles. LCCs are hardened to 2,000 psi.

In addition to regular cable connections, since 1990, the LCCs have been equipped with terminals for batch satellite connections through the Defense Satellite Command System (DSCS). When the DSCS ends its term of service in 2003, the LCCs will be integrated into the MEECN communications system, which will allow them to receive commands and relay them to missiles through the satellite channels of the MILSTAR system in EHF and VLF/LF ranges. New EHF terminals will replace the existing Super High Frequency Satellite (ISST) terminals and the AFSATCOM system equipment of the, while new VLF/LF terminals will replace the Survivable Low Frequency Command System (SLFCS) terminals. Existing and new terminals are HEMP protected.

(http://www.fas.org/nuke/guide/usa/C3i/icbm-lcc.htm)

4.3.2 Communication and Control Systems

4.3.2.1 – Global Control System: from WWMCCS to GCCS

In the early 1960s, the United States set out to create a single global system for command and control of its widely dispersed forces (Worldwide Military Command and Control System – WWMCCS). The goal of the system was to allow the transfer of information to any location and at any level of command within minutes. By the late 1960s, about 160 different computer systems with 30 different general-purpose software systems were used at 81 locations.

Due to technological problems and financial limitations, however, the WWMCCS was never realized to the full potential envisioned for the system. Its shortcomings brought about several serious fiascos. In June of 1967, for example, during the Arab-Israeli conflict, the USS *Liberty*, a naval reconnaissance ship, was ordered by the JCS to move further away from the coastlines of the belligerents. Five high-priority messages to that effect were sent to the *Liberty*, but none arrived for more than 13 hours. By that time the ship had become the victim of an apparently mistaken attack by Israeli aircraft and patrol boats that killed 34 Americans.

The system was gradually upgraded, and, on the whole, provided a range of capa-

bilities appropriate for the diverse needs of the WWMCCS sites. In particular, it made possible the Desert Shield and Desert Storm operations. However, in view of the high operation costs of the system and its failure to match growing demands, the WWMCCS was officially deactivated in August 1996, in favor of a new global control system – the Global Command and Control System (GCCS).

The GCCS is an automated information system designed to support deliberate and crisis planning with the use of an integrated set of analytic tools and the flexible data transfer capabilities. GCCS will become the single C^4I system to support the warfighter from foxhole to command post. The C^4I for the Warrior (C^4I FTW) concept, already in action today, is committed to the challenge of meeting the warrior's quest for information needed to achieve victory for any mission, at any time, and at any place.

The Global Command and Control System (GCCS) involves all of the military organs, including the Department of Defense, the JCS and the STRATCOM. It addresses questions of planning and conducting operations, mobilization, deployment, employment, sustainment, and intelligence. The organs and channels of nuclear control are integrated into the GCCS for carrying out specific tasks as well as with regard to many general questions.

(http://www.fas.org/nuke/guide/usa/C3i/wwmccs.htm)
(http://www.fas.org/nuke/guide/usa/C3i/gccs.htm)

4.3.2.2 – The National Communications System

The U.S. nuclear control system is also integrated into the National Communications System (NCS). The 23 members of the organization are tasked with ensuring that the federal government has the necessary communications under all conditions from normal situations to national emergencies and international crises. The current 23 members include departments and agencies like the Department of Defense and the JCS.

When necessary, authorized teams from all members of the system meet in locations designated and arranged ahead of time and prepare coordinated recommendations for the liquidation of the consequences of the crisis.

During these emergencies the NCS provides necessary communications resources. In particular, under the Shared Resources High Frequency Radio Program (SHARES), radio resources belonging to 53 federal and federally affiliated organizations are made available. The SHARES network consists of 1,040 HF radio stations located in the United States and abroad and over 250 HF frequencies.

(http://www.fas.org/nuke/guide/usa/C3i/ncs.htm)

4.3.2.3 – Minimum Essential Emergency Communications Network

The U.S. nuclear control system relies on the Minimum Essential Emergency Communications Network (MEECN). The main goal of the MEECN is to ensure that the

president can send Emergency Action Messages (EAMs) to the National Command Authorities and the Strategic Nuclear Forces.

Several outdated programs remain in the MEECN at the "sustainment" stage and should be deactivated. In particular, this is the Ground Wave Emergency Network (GWEN), which does not match current operational and survivability demands. The American C³ network is increasingly relying on satellite forms of communication.

The MEECN is upgraded through three basic projects:

- DIRECT (Defense IEMATS Replacement Command and Control Terminal): switching from the AUTODIN system (see 4.3.3.1), which had served out its term of over 30 years to the Defense Message System (DMS);
- ILES (ICBM LCC EHF) or simply EHF: equipping ground missile LCC terminals with terminals for two-way communication with country's highest authorities;
- Modified Miniature Receive Terminals (MMRTs): installation of MMRTs operating at very low frequencies onto B-1 and B-52 fighter planes, LCCs, and airborne command centers to allow for communication with the NCA. Along with the miniaturization and unification for the various consumers mentioned, these receivers are better protected in emergencies.

4.3.2.4 – Strategic Automated Command Control System – (SACCS)

The main purpose of the SACCS is to provide command and control of the nuclear missile forces. Through the system, the STRATCOM receives Emergency Action Messages (EAMs) and Force Direction Messages (FDMs) from the supreme commander and relays them to its subordinates. The system also provides situation monitoring, warning, strategic planning and retargeting, and damage/strike assessments.

SACCS terminals are located at STRATCOM command centers and all subordinated command centers down to the LCS, launch control facilities and strategic aircraft sites. This system also provides SIOP messages to Air Combat Command, Air Mobility Command, Air National Guard and Air Force Reserve for the deployment of strategic fighter planes, mobilized aircraft and refueling aircraft.

The SACCS network also serves six external interfaces: Data Processing Subsystem (DPS), Air Force Global Weather Center (AFGWC), Command Center Processing and Display System (CCPDS), AUTODIN, Air Force Satellite Communication (AFSATCOM), and 616A (a survivable Low Frequency Communications System).

The system was first procured by the Strategic Air Command (SAC) in 1963. In 1988, it was upgraded and renamed the 465L SACDIN (SAC Digital Network). The SACDIN was able to maintain an end-to-end message delivery time of not more than 15 seconds for an Emergency Action Messages. Total system cost for SACDIN (SAC Digital Network), including a later modification, was nearly $1 billion. After formal acceptance, the system became known as SACCS. (The systems used to provide command over U.S. nuclear submarines include ELF, VLF, and TACAMO.

(http://www.fas.org/nuke/guide/usa/C3i/saccs.htm)

4.3.2.5 – Extremely Low Frequency Communications Program (ELF)

The range used for ELF is 40-80 Hz. The first ELF experiments used a 220-kilometer antenna mounted at Laurentian Shield, Wis. Then, a 45-kilometer antenna was tested at Clam Lake, Wis. Finally, despite serious opposition from environmental activists, a transmission center with a 90-kilometer antenna was set up at an air force base in Michigan.

In 1985, the center began transmitting commands to submarines in the Pacific Ocean, and then to submarines in the Mediterranean Sea and the Northern Polar Ice Cap.

(http://www.fas.org/nuke/guide/usa/C3i/elf.htm)

4.3.2.6 – Very Low Frequency (VLF)

Ten powerful VLF/LF transmission centers located throughout the world broadcast commands from the NCA in the Very Low Frequency and Low Frequency ranges (14-60 kHz). Each center simultaneously broadcasts through four 50bps channels.

Until recent times, the centers used outdated (40-year-old) technology, which employed vacuum tubes. Right now, under the SSPAR program, the transition to solid-state technology is underway.

The website cited below provides data from some of these facilities:

NPM Lualualei, Hawaii	21,4 kHz	480 kW
NAA Culter, Maine	24,0 kHz	750/1000 kW
NLK JimCreek, Wash.	24,8 kHz	192 kW
NAU Aguada, Puerto Rico	40,75 kHz	100 kW

(http://www.fas.org/nuke/guide/usa/C3i/vlf.htm)

4.3.2.7 – TACAMO System

The Take Charge and Move Out (TACAMO) system provides communication with submerged submarines through specially equipped aircraft. Two E-6A "Mercury" class squadrons – the "Ironmen" and the "Shadows" – deploy more than 20 aircrews from Tinker Air Force Base, Okla. These aircraft replaced the aging EC-130Qs. The Air Force received the first E-6A in August 1989.

The current 200-kilowatt transmit sets on radio relay aircraft are currently being replaced with the new, more powerful, High Power Transmit Sets, which use very low frequencies. The antenna is a dual trailing wire assembly type, about 8 kilometers in length. Since it is more effective the more vertical it is in flight, work to fine-tune this

aspect of the project is underway. The E-6, based on the Boeing-707 commercial airplane, has a crew of 14, a total weight of 154 tons, a ceiling of 13 kilometers, a maximum speed of 960 kph, a range of 12,000 kilometers and costs 141.7 million dollars.

(http://www.fas.org/nuke/guide/usa/C3i/e-6.htm)
(http://www.chinfo.navy.mil/navpalib/factfile/aircraft/air-e6a/html)

4.3.2.8 – Military, Strategic, Tactical and Relay (MILSTAR) Satellite Communication System

MILSTAR is currently the most technologically advanced military communications system. MILSTAR terminals are installed on almost all command posts and nuclear missile carriers. It is a large and very expensive system that has several stages of development, including the three basic ones: MILSTAR1, MILSTAR2 and MILSTAR3.

MILSTAR1:

The MILSTAR program was first developed in the early 1980s to provide secure command over U.S. strategic and tactical nuclear missile forces in case of nuclear war. The original plan included the creation of a group of nine satellites: four active and one reserve satellites in geosynchronous equatorial orbit, and three active and one reserve in geosynchronous polar orbit. The total cost of the program, including ground equipment was estimated at $22 billion, with each spacecraft costing about $800 million.

With the end of the Cold War, however, in 1991, the Congress seriously limited financing for the program. The program was changed to consist of six satellites in a mixture of low- and high-inclination orbits. The first MILSTAR1 satellite was launched in early 1994, with the other satellites launched at a rate of one a year. Each satellite weighs about 4.5 tons, has a design life of 10 years and solar panels that generate 8,000 watts of power. MILSTAR terminals were first installed for the nuclear forces, and then for other purposes.

(http://www.fas.org/spp/military/program/com/milstar1.htm)

MILSTAR2:

With the end of the Cold War, the satellite communication system was expected to reorient from serving strategic nuclear to serving conventional (tactical) forces. There were also increasing demands to reduce system costs. In parallel with the MILSTAR1 program, a new program, MILSTAR2 was introduced, to fulfill these demands.

The classified payload was removed from MILSTAR2 satellites; spending on the "Heroic" survivability was reduced; the reduced functions of nuclear forces command were replaced by functions of tactical forces command; the cost of ground terminals was cut by 35 percent.

MILSTAR2 is a constellation of four satellites. The first one was launched in the late 1990s. The group was slated to be replenished between 2006 and 2009. Therefore, under the plan, nine such satellites were to be purchased by 2011.

On April 30, 1999, the Titan missile that was launching the third satellite entered an orbit that was lower than planned. As a result, the satellite went into a wrong orbit, and was declared a complete loss on May 4, 1999. Nonetheless, MILSTAR2 launches were continued. According to official U.S. estimates, about $12 billion was spent on the MILSTAR program between 1994 and 1999.

(http://www.fas.org/spp/military/program/com/milstar2.htm)

MILSTAR3:

The new stage of the program, the Advanced Extremely High Frequency (AEHF) program, is also a constellation of four satellites that cover the globe from 65 degrees north to 65 degrees south. The system will now have a more general name – AEHF MILSATCOM, or advanced extremely high frequency military satellite communication, although this is probably mainly a technical name. (Apparently, the U.S. military has so many command and communications systems, it is easier to use "technical" names.)

The capabilities of the new generation of MILSTAR will be significantly higher, but, at the same time, the cost of the system has been decreased again. The total value of MILSTAR3 is estimated at "only" $2.5 billion (including ground equipment). The first satellite of the series is expected to be launched by December 2004.

In light of the "multilayered" nature and high cost of the MILSTAR system, Americans pay a lot of attention to the optimal combination of its stages, preemption, etc. Under the current plan, MILSTAR1 and MILSTAR2 will be continued, but the MILSTAR2 constellation will not be replenished with its own satellites (accordingly, satellites will not be built as planned). Instead, starting in 2005, the MILSTAR3 system will be deployed in full. However, debates about the optimal transition period continue.

(http://www.fas.org/spp/military/program/com/milstar3.htm)

4.3.2.9 – Concept for the development of satellite communication

This concept is provided in the U.S. Department of Defense program, "Space Communications Architecture." Under this program, the future (2010-2025) system of military satellite communication must:

- provide direct connections to any recipient, at any time and at any place;
- be fully integrated into the existing network of military information systems;
- have minimal "footprints" – overt signs of terminals, antennas, etc.

Extensive international cooperation is considered one of the main conditions for the

creation of such a system.

Technologically, this global system will consist of the EHF, X/Ka band, UHF, and Polar System subsystems.

The EHF Satellite System will replace MILSTAR, improving channel capacity to six to eight, and later 10 and more, megabytes a second, which should improve interference protection.

The X/Ka Satellite System will replace the current Defense Space Communications System (DSCS) and the Global Broadcast System (GBC). The main advantage of this system will be the increased volume of the communications on the network, i.e., the number of recipient channels. This project, like many others, will use commercial-like developments.

The UHF Satellite System will address the problem of secure communications with various mobile objects. It is believed that current commercial developments are not sufficient, but they will be used as well.

The Polar Satellite System will be used for communications with objects located above 65 degrees north. The launch of a low-capacity EHF system into a high-inclination orbit is being considered. 24-hour coverage will require two such satellites.

Overall, the architecture listed above will have a maximal unification of ground terminals, and an integrated observation and control network for the satellites.

(http://www.fas.org/spp/military/program/com/)

Almost all of the aforementioned sites have references to other sources. Through them, it is possible to receive more comprehensive information about specific projects. Since many of the indicated sources have illustrations, diagrams and tables, the author found it practical not to offer them in this book. The www.stratcom.mil site provides information about STRATCOM and the forces it commands. It also offers the biographies of the commanders, including C⁴ (command, control, communications, and computer systems) Director, Brig. Gen. Emile Bataille. The main publications of the organization, various statistics and links to other sites are provided.

A lot of information related to command of American nuclear forces can be found on the websites of the U.S. Department of Defense. One can easily access it through www.defenselink.mil/ sites. This web page provides the addresses of 30 primary sites, including the Air Force, Army and Navy; the Department of Defense, the Joint Chiefs of Staff and the Pentagon; NORAD and NATO; and the U.S. Congress. About 1,000 other sites are listed that have information on almost all spheres of military affairs, including data from the military budget, new technologies, and development and purchasing of various armament systems.

Below, the information on military satellite communications from the website of the Federation of American Scientists is provided as an example.

1) http://www.fas.org/spp is the website of the Federation of American Scientists organization (fas.org) Space Policy Projects (SPP) section.

2) The SPP section includes a "military" projects section along with civilian U.S.projects and international projects. http://www.fas.org/spp/military.

3) The military section includes a guidebook of the Department of Defense on military technology; a report of the Commission to Assess United States National Security Space Management and Organization; facilities; doctrine, exercises and operations; budgets; materials of congressional hearings; reports from the General Accounting Office; space agencies; and finally the "Programs" section: http://www.fas.org/spp/military/program.

4) The "Programs" section includes navigation, meteorology, etc., including a subsection on communications: http://www.fas.org/spp/military/program/com.

5) Here one can find information on any operational satellite communications system or a project under development in the given area. If the name of the desired project is known, it can be found directly – for example: http://www.fas.org/spp/military/program/com/milstar3.

4.3.3 The General Algorithm of American C^3

There is not a lot of general information about the algorithms of the U.S. nuclear command system in the sources reviewed. This may be because they are different in every case and depend on the specific task: either the command system functions in emergencies, bringing forces into a certain level of battle-readiness; or it is the day-to-day operations of headquarters and forces; or the C^3 elements that survive an enemy attack secure a retaliation attack, etc. The most interesting situation is the way the system is supposed to work after receiving information about the start of a missile attack against the United States from the Early Warning (EWS) system. In other words, the algorithm of the launching function of U.S. C^3.

Based on information from open sources, including those listed above, the following picture is created:

A signal from the Cheyenne Mountain Complex is sent to the U.S. president, the secretary of defense, the STRATCOM command centers, and other joint command centers. After a short teleconference, if a decision to retaliate is made, the National Command Authority uses the "Football" to give a battle action order to the nuclear missile forces (an EAM signal with launch codes). At the same time, the U.S. population is informed through the EAS system. Reserve command posts, including the airborne command posts of the NCA (E-4B NAOC) and STRATCOM (E-6B) and mobile consolidated command centers of STRATCOM and SPACECOM (MCCCs)

LIST OF ADDITIONAL C³ SYSTEMS AND PROJECTS ON THE INTERNET

AUTODIN
http://www.fas.org/nuke/guide/usa/C3i/autodin.htm
AUTODIN System – now being replaced after serving for over 30 years.

FEMA
http://www.fas.org/nuke/guide/usa/C3i/dcwcs.htm
System for the Federal Emergency Management Agency (FEMA).

DMS
http://www.fas.org/nuke/guide/usa/C3i/dms.htm
The new DMS communications system that is replacing AUTODIN.

DIRECT
http://www.fas.org/nuke/guide/usa/C3i/direct.htm
DIRECT program to replace AUTODIN with the new DMS.

National Emergency Alert System
http://www.fas.org/nuke/guide/usa/C3i/eas.htm
Provides emergency information to the population in the case of an emergency through AM/FM radio and television broadcasts.

Combat Ciders
http://www.fas.org/nuke/guide/usa/C3i/combat_ciders.htm
Subsystem of the BBC radio broadcasts, and element of the AUTOVON system.

HF Buoys
http://www.fas.org/nuke/guide/usa/C3i/an-bst-1.htm
HF transmitter on two buoys for urgent reports to shore from a Trident submarine. Renewed in 1988.

Voice Command
http://www.fas.org/nuke/guide/usa/C3i/ercs.htm
The system for voice commands to LCCs through command missiles from 1961 until the early 1990s.

Low Frequency
http://www.fas.org/nuke/guide/usa/C3i/fsbs.htm
Modernization of the system for transmitting commands to submarines in the Low Frequency range through the reduction of the number of shore stations.

GWEN
http://www.fas.org/nuke/guide/usa/C3i/gwen.htm
Ground Wave Emergency Network (GWEN) system of low frequency transmission stations for improving the interference protection of emergency communications. The service is ending.

Joint Planning and Implementation
http://www.fas.org/nuke/guide/usa/C3i/jopes.htm
National system of joint planning and implementation, which includes the STRATCOM.

Reserve Air Force System
http://www.fas.org/nuke/guide/usa/C3i/mystic_star.htm
Reserve system of radio communication with Air Force bases throughout the world.

Alternate Communication Center
http://www.fas.org/nuke/guide/usa/C3i/raven_rock.htm

C^3 sytems Internet citations cont.

Survivable Low Frequency Communication System
http://www.fas.org/nuke/guide/usa/C3i/slfcs.htm

National Military Communication System
http://www.fas.org/nuke/guide/usa/C3i/nmcs.htm

Satellite Communication System for Submarines
http://www.fas.org/nuke/guide/usa/C3i/ssixs.htm

Cable Military Communication Network
http://www.fas.org/nuke/guide/usa/C3i/tcs.htm

Digital Very Low Frequency Information Network
http://www.fas.org/nuke/guide/usa/C3i/verdin.htm

are activated. The reserve command centers are authorized to act if the primary command centers are disabled. The TACAMO E-6A aircraft system is activated and deployed. The crews of submarines are informed through this system and other long wave (ELF and VLF) radio communication systems.

Commands from the NCA and STRATCOM, including missile launch commands, are transmitted to the ICBM launch control centers (LCCs), strategic fighter planes, shore and air transmission stations simultaneously through all available communication systems (GCCS, SACCS, SLFCS and others) using cable (TCS), short wave (HF, UHF), long wave (VLF) and satellite (MILSTAR, AFSATCOM and other) channels. The end-to-end message delivery time to missile launch does not exceed one minute. Minutemen-M and M-X missiles are launched by LCCs; however, if the LCCs are disabled, remaining missiles can be launched by E-6B aircraft through the ALCC terminals described in section 4.3.1.9. Submerged submarines receive orders through ground (ELF, VLF) and air (TACAMO) transmission centers. Fighter jets in the air (and on the ground) are controlled through short-wave and satellite channels. The algorithm provided can vary depending on the initial state at the time the signal about the beginning of a missile attack against the United States is received. If the signal is preceded by a crisis situation, the C^3 system will be better deployed and more combat ready than in case of a sudden large-scale attack. However, most experts consider the second scenario even more unlikely than the first.

It is known that significant changes were made in the structure of the high military command of the United States after Oct. 1, 2002. A new joint command center (NORTHCOM) has begun functioning under Air Force Gen. Ralph E. Eberhart, who was previously the head of SPACECOM. This has, to some extent, affected the nuclear missile command system. However, this fact does not change the essence of the information provided or the goal of the given work: to show the extent and character of open information on the U.S. C^3.

4.3.4 Problems

Operational planning is the most difficult area for unclassified analysis of nuclear weapons C^3. This does not refer to specific strike plans with a list of targets; such data is unnecessary for the purposes of this book. But it would be useful to be able to assess the flexibility of weapons use and the different systems in specific situations. Because this information remains highly classified, however, it is only possible to evaluate these kinds of American and Russian C^3 capabilities indirectly from some American sources.

American experts emphasize that the type and functions of a C^3 system are greatly dependent on the content of operational plans:

> "... These actions, all of which would have compromised safety, flowed from the requirements to be ready and able to destroy a huge number of Soviet targets. In 1986, for example, SIOP forces were assigned 16,000 individual Soviet targets."[165]

They further note that the extremely high degree to which Soviet C^3 was centralized guaranteed great strategic flexibility, by allowing the country's leaders to participate directly in combat decisions rather than just to authorize a plan established in advance. On the other hand, this system, in view of some of these experts, made it more difficult to carry out plans rapidly and effectively:

> "Soviet targeting policy for intercontinental ballistic operations appeared to emphasize flexibility. The nuclear command and control system was expected to conform to the wishes of the supreme high command, which might demand a menu of options. High-ranking Soviet political officials often participated in nuclear exercises. In a real conflict, they were expected to manage nuclear operations in a detailed way, not simply to endorse preexisting plans for all-out attack. In short, the Soviet command system was not rigid but flexible in developing a course of action, though it appeared quite rigid and ponderous in carrying out the plan. By contrast, the U.S. command system was agile in carrying out an intricate pre-established plan but appeared quite inflexible in supporting a novel course of action."[166]

It is hard to confirm or deny this assessment. Frequent participation by Soviet leaders in nuclear force exercises is probably an exaggeration. They sometimes attended field tests of new missiles and pushed a launch button, but this hardly constitutes real involvement. The Soviet leaders, as mentioned earlier, never took part in any exercises with the "nuclear briefcase." But the quotation above is certainly true for the highest military leadership of both the U.S.S.R. and now – the Russian Federation, especially

at the level of three SNF legs commanders. These leaders knew and still do know virtually all the operational "fine print" of C^3 use, and are able to advise political leaders of various options in a timely and clear fashion.

But what about the apparent trade-off between flexibility in planning versus rigidity in execution that is described as characteristic of Soviet/Russian C^3? The system is technically capable of storing and quickly selecting among a number of action plans sufficient to allow for all reasonable conflict scenarios. How many plans there are, and what they consist of at any given time, is another question. This is, so to speak, "variable" information. The description of Russian C^3 in a previous chapter makes it clear that a specific missile launch plan takes only minutes to execute, and (technically) may be done in assigned time intervals. Thus, it is not clear what the American writer quoted above had in mind. On the other hand, the supposed rigidity of the American system in "supporting a novel course of action" may be equally questionable.[167]

In a time of crisis, besides the "minimal" MEECN network, all American peacetime communications would be brought into play, primarily using rented cable channels and parts of the national public communications systems. On the whole, such a system provides for stable management of U.S. nuclear forces. A number of American experts, however, have *expressed doubts* about reliability of the system's separate parts. They note its vulnerability to a high-precision conventional or tactical nuclear strike, much less a hit by a powerful Russian ICBM. The radio channels on which all airborne command posts rely are sensitive to interference and ionospheric disturbances caused by ground and especially high-altitude nuclear explosions. Great attention is also paid by Americans to the dangers of electromagnetic pulse (EMP) weapons.

American sources describe previous mistakes of missile early warning system:

"It should also be noted that U.S. early warning system have a credibility problem that bears on their utility for warning of a Soviet attack. Occasional false reporting by the U.S. early warning system has resulted in unnecessary nuclear alerts, as in the incidents of June 3 and 6, 1980, when erroneous warning of incoming Soviet SLBMs and ICBMs resulted in the scrambling of SAC strategic bombers."[168]

Pry describes some other design faults: a missile cannot be launched using the crews of only one LCC; two crews working together are needed for a successful launch. If, during combat, four of five LCCs in a squadron become inoperable, none of the 50 missiles will be launched. There is no technical capability for a neighboring squadron to take over the launch of those 50 missiles. ALCCs are described as no more than "a temporary means of controlling ICBMs."[169]

"ALCCs can launch missiles only when flying within sight of the wing. ALCCs cannot remain airborne forever, but must land periodically for maintenance and refueling. ALCCs can be maintained on station most days if tanker support is available, but only for hours if there are no or too few tankers for continuous refueling."[170]

Blair draws some comparisons between the airborne elements of the Russian and U.S. C^3 systems for direct transmission of a launch order to the missiles.

> "Soviet SRF officers indicated that their airborne command posts could remotely fire (at a range of about 200 miles) an ERCS missile, which in turn could transmit the firing signals directly to the unmanned ICBM launchers. One such source further indicated that the airborne command posts were able to transmit fire signals directly to the ICBM launchers in special circumstances, but that the procedure was extremely complex and could be performed only when coordinated with the activities of other launch centers.
>
> For the United States, airborne launch control centers were the primary backups to the underground launch control centers. In a crisis, airborne launch control centers would have initiated patrols in each of the six regions of Minuteman deployments to back up the ground crews. Some but not all of these SAC aircraft possessed all the codes necessary to issue valid launch orders to the ground crews, replete with unlock codes. They could also have bypassed the ground crews and sent fire signals directly to the unmanned silos after a high alert was declared. Safeguards on board the aircraft were largely procedural, except for that portion of the airborne fleet that acquired unlock codes only upon receiving a launch message from higher authority."[171]

In theory, the major command and communication aircraft are hardened against EMP, but no one can predict how this protection will actually work when put to the test. Such hardening can also cost up to 20 percent of the total expenditures for a protected aircraft, so that protecting one NEACP aircraft against EMP can run about $100 million.[172]

Some experts believe that American C^3 is not designed to win a protracted nuclear war. Even though the system's logical components (i.e., computers) are sufficiently flexible to provide operational options for such a war, the physical components (primarily command posts and communication channels) do not have the necessary survivability. Various sources describe other such defects.[173]

Two points in particular concerning American C^3 are important to the purposes of this paper. First, the American system's components and functions are similar to those of its Russian counterpart. Any attempt, however, to try to determine whether one side "borrowed" from the other would be pointless. Technical and doctrinal similarities between the systems arise from the very nature of nuclear weapons themselves and the ideas that govern their proposed use; each country arrived at its present C^3 configuration independently and inevitably. There are, nevertheless, certain differences in U.S. and Russian approaches to using C^3. One example is the way survivability of the system is ensured. Americans have chosen to emphasize mobile components – land-based and airborne – while Russia has, besides those, traditionally paid greater attention to hardened underground command posts.

The second point lies in the *relative* nature of such concepts as "strong" and "weak" when applied to U.S. C^3 by American experts. Such qualitative evaluations lie very much in the eye of the beholder. It is possible to keep investing huge sums of money in C^3 and achieve nothing. It is more important at the present time to evaluate scientifically how C^3 systems contribute to the general goal of strengthening strategic stability. Short of this, it remains clear that Russian and American C^3 systems are reliable enough to avoid starting a nuclear war.

As for problems of U.S. C^3 development, American experts cited earlier the enduring indifference to C^3I problems among those responsible for allocating defense funds. Everyone paid lip-service to the system's importance, but the reality was quite the opposite. Even when C^3 development was declared to be an official goal, actual changes remained insignificant. Blair describes how the Reagan administration declared development of C^3 the main goal for updating nuclear forces: "According to Reagan, modernization of the control system was crucial to the success of the overall plan;" without dependable C^3I, new weapons cannot be transformed into effective power. Support for this thesis continues to run deep and wide. The Scowcroft Commission expressed a representative opinion: "Our first defense priority should be to ensure that there is continuing, constitutionally legitimate, and full control of our strategic forces under conditions of stress or actual attack. ... The Commission urges that this program continue to have the highest priority."[174]

In reality, however, legitimate doubts were voiced about at least three aspects of C^3I: goals; technical feasibility; and funding. The lack of clear goals arose from undefined priorities in the strategic concepts of nuclear weapons use. Scott D. Sagan, a leading American expert in this field, explained the title of his book on nuclear strategy: "*Moving Targets* does not refer only to mobile missiles ... It is also an allusion to the central topic ... Indeed, as anyone who has written about this exceedingly complex subject understands, U.S. nuclear strategy, in many ways, is itself a moving target."[175]

Doubts about the possibility of developing a C^3 system that would satisfy serious prospective requirements arose from a major technological challenge facing scientists and engineers. It was impossible to predict behavior of the opposite side, for decades in the future: "Defense officials seem keenly aware that a technological challenge of daunting dimensions accompanies the goals laid out by the Reagan administration."[176] A number of well-known Western experts did not believe in an "ideal" system: "Among others who do not share the administration's sanguine view are Desmond Ball and John D. Steinbruner. Ball concludes that 'the capability to exercise strict control and coordination would inevitably be lost relatively early in a nuclear exchange ...' In this same vein, Steinbruner contends that a dependable technical solution to C^3I endurance probably cannot be achieved at feasible cost."[177]

Most experts agreed only on the need to increase the survivability of C^3 in the initial stage of a nuclear exchange, and supported funding requests for these improvements. What funding the administration did end up allocating for C^3 went mostly to R&D,

not to manufacturing and deployment. Blair noted that some promising C^3I developments found a temporary refuge in R&D, but it was not clear whether the results of such research would ever be implemented.

Time has shown these fears to be well founded. By the mid-1980s, production was assured only for some of the system's components. Even the most successful developments remained underfunded, and the dramatic increase in funding promised by the administration never materialized. Blair complains that as in the past, C^3 received only 1.5 percent of the defense budget, or about 10 to 12 percent of the total strategic nuclear forces budget. He points out that, from 1970 to 1985, the United States annually invested an average of $1.5 billion for development of command, control, communication and tactical early warning.[178]

Unfortunately, the data on funding for command and control varies widely among U.S. publications. For example, a different source claims: "Between 1977 and 1986, funding for C^2 equipment jumped nearly 150 percent, from less than $10 billion annually to nearly $25 billion a year, as computers, communications systems, and surveillance systems acquired status comparable to the most advanced bombers and submarines."[179] These differences in data may be a result of the many rather free interpretations of what constitutes command and control: C^2, C^3, C^3I, or C^4I?

In comparison to the problems of Russian C^3, such a budget share (10 to 12 percent), is not so small (especially if one takes into consideration the absolute size of defense spending in the United States). In the 1970s, the Strategic Rocket Forces were well ahead of the other nuclear triad forces in command and control. During this period the Strategic Rocket Forces command earmarked up to 15 to 20 percent of incoming revenue for the development, manufacture and deployment of the *Signal, Vyuga, Perimetr,* and other systems. At the same time, missile development continued apace, and even showed some increase.

In both the United States and Russia, however, there has been a clear trend toward redistributing funds officially allocated for C^3 into weapons systems. Even though C^3 is an integral part of these weapons, it still does not receive adequate support. "That weapons systems are the main beneficiaries of the administration's defense largesse is further suggested by the fact that key C^3I programs such as the E-4B airborne command post and ECX TACAMO were scaled down or stretched out during Reagan's first term."[180]

Low funding levels for C^3 (C^4I) may also be due to the fact that the nuclear triad is the "cheapest" part of the armed forces, and that defense spending levels in general have been decreasing. In 1995, the then Strategic Rocket Forces Commander in Chief Col. Gen. Igor Sergeyev noted: "The spending for developing and maintaining SNF is only 10-15percent of the total military budget; as for the Strategic Rocket Forces – the main component of SNF – it's no more than 5 to 6 percent."[181]

It would be logical to increase spending gradually on C^3 for strategic nuclear forces as force levels themselves decrease. This notion seems slowly to be taking hold in the United States, as recent C^4I programs are given high priority and financing.

In his book, "Weapons Acquisition in the Soviet Union," Stan Woods makes an interesting comparison between weapons R&D in the Soviet Union and the United States: "Three groups play a major role in the weapons acquisition process in any society: the military (with their doctrines, history and traditions), the political leadership (with all of its priorities, values and aspirations), and the R&D community combined with the defense industry as a whole. The production of new weapons is not the result of a rational progression of events but is the output of a complex web of iterative relationships among these groups."[182]

This describes, for the most part, the situation today both in Russia and the United States. So far chief designers of weapons are more successful than their C^3I colleagues in convincing the powers that be that their "products" are the most "essential" for national security. This situation is partially due to the absence of commonly recognized authoritative methods for substantiating the contribution of each element of nuclear forces into the general result (deterrence).

There are three distinctive types of problems in the ongoing, often political, fight over the future development of American C^3I. First is the need to ensure that the system will function reliably during the first few minutes of a nuclear conflict, under conditions of launch-on-warning before the enemy's warheads reach their targets. While these problems have been given sufficient financial and technical attention, there is a critical aspect that remains not addressed: "... it is not comprehensive and slides past the issue of whether a responsible, considered decision is humanly and organizationally possible when there are only a few minutes to decide."[183]

The second issue is how the command and control system functions in the first few hours of an enemy attack. The network of airborne command posts and communication centers is the anchor of this system and its further development continues to be partially funded. Despite financial and technical challenges, the "airborne concept" is still considered viable as "insurance" for the less reliable ground-based components of C^3.

The third group of problems deals with a protracted war. These problems never have been explored thoroughly, and their study remains essentially unfunded. There are exceptions to this rule, such as the project for creating a system (the Integrated Operational Nuclear Detection System – IONDS) that would discover and analyze nuclear explosions from space, both in the United States and other regions. IONDS potentially would be able to assess the damage to each side in a conflict, and then use that information to change plans for subsequent employment of the remaining nuclear forces. The system is projected to have up to 18 satellites, with high operational autonomy (no ground support), and the ability to deliver information directly to the user.

Other C^3I programs with high potential are to:

- increase the survivability of EWS satellites;
- develop mobile ground-based terminals for the EWS;

- upgrade BMEWS radars;
- improve the survivability of airborne command posts against the effects of nuclear explosions;
- increase the survivability and operational capability of stationary command posts;
- develop alternative satellite communications systems alongside MILSTAR;
- expand ELF submarine communications.

All of the above measures are well known from the theory and practice of military and civilian communications. These ideas have been researched and developed at the institutes, laboratories, and testing ranges of Russia, France, China and elsewhere. The choice of specific technologies depends on each nation's technical and financial means. Blair rightly points out, "Strategic analysis has long suffered from a methodological affliction known as the law of the instrument, which states that problems must be tailored to the tools at one's disposal."[184] At the same time, however, he notes the lack of a clear methodology for assessing the contribution of C^3 systems to strategic stability. This lack is directly responsible for the already mentioned financial emphasis on weapons systems alone.

"Because available tools are generally honed for problems that can be readily quantified, rigorous assessment has steadily advanced, but in narrowly circumscribed areas of interest: the size, technical composition, and economics of nuclear weapons. Progress toward assessing the central question – command system performance – has not been commensurate. Standard calculations, in fact, have obscured the problem of force management, a subject that generally defies meaningful quantification."[185]

The situation is the same in Russia today. The "law of the instrument" is hardly a useful way to approach serious problems with any hope of success. In the case of C^3I, it prevents researchers from discerning true priorities and concentrating resources on solving them.

4.3.5 Some Personal Observations

A lot of interesting information was kindly given to me during a visit to Offutt AFB, to which I was invited as an independent expert on Sept. 11-12, 1996. With the help and cooperation of Alfred A. Buckles, principal deputy J-6 (C^4I systems), I was fortunate to see things I had been able only to imagine when I served in the Soviet Rocket Forces and at the General Staff. At Offutt, I listened to a presentation on the underground command post while sitting in a commander in chief STRATCOM chair, from where American nuclear forces would be directed in a crisis. I talked with enlisted personnel and officers on duty in a Looking Glass plane. I saw the president's Airborne Command Post, the TACAMO plane and many other interesting things. My hosts naturally were not able to inform me about everything I was interested in, but what I did learn was enough to form a general picture and draw some conclusions.

The USSTRATCOM in Omaha is, on the one hand, a well-tuned, smoothly func-

tioning mechanism staffed by highly skilled professionals who are ready at any given moment to work at any command post. On the other hand, USSTRATCOM's personnel are a team of intellectual, friendly, happy people who seemed surprisingly similar to Russians. Sometimes, I felt I was in a Soviet missile division in Siberia once again, the atmosphere was so familiar. When saying goodbye, we all expressed the wish that we never would have a reason to put the capabilities of our command posts at Omaha and Perkhushkovo to the test.

Chapter 5

Problems with Russian and U.S. C^3

This chapter deals with certain comparative problems in the structure and operation of Russian and U.S. nuclear C^3 systems. It provides a brief analysis of some problems common for both sides. This analysis is organized around the author's comments on published views of American specialists.

Nuclear C^3 systems are essentially inertial: substantial changes in these systems take place relatively slowly, over many years. The main trends in their development are long-term in character, and their fundamental characteristics have been practically immutable since the invention of nuclear weapons. Therefore, I will refer in this chapter to sources dating from the 1970s and 1980s to most recent ones. From the point of view of this book, which makes an argument for international cooperation of C^3 experts, such a time frame is quite appropriate.

5.1 Negative Control

Russia's nuclear C^3 system is viewed by the majority of foreign and domestic experts as one of the most protected against unauthorized actions: "Although unforeseen loopholes lurk in any system, a long-standing and deep-seated obsession with controlling nuclear weapons led the Soviets to go to extraordinary lengths to ensure tight central control on nuclear weapons. Their safeguards were more stringent than those of any other nuclear power, including the United States."[186]

All organizational and technical measures of negative control were unified in the Soviet/Russian C^3 system under a program known as "*Zashchita*" (Protection). The General Staff has the exclusive prerogative for the implementation and improvement of this system. The main staffs of the nuclear triad components are responsible for the implementation of concrete orders from the General Staff in their subordinate forces.

5.1.1 Lower Levels of Russian C^3: Below the Top Leadership

Blair describes this complex system in the following way:

The main safeguards:

1. the division of the command and control structure into two distinct types of organizations with separate chains of command, one responsible for managing the technical state of nuclear forces and one for providing military direction to the combat units;

2. the standard practice of keeping nuclear warheads apart from their delivery units;
3. the application of two-person rule;
4. the utilization of elaborate feedback loops that enable subordinate units to be closely monitored by higher echelons;
5. the extensive use of electronic systems that enable higher echelons to disable missile launchers quickly and to neutralize lower level command posts;
6. the extensive use of blocking devices designed physically to impede the unauthorized use of weapons.[187]

In general, this description is correct. A brief commentary with respective numerical reference is in order.

1. Russian C^3 is characterized by a clear division of command and control functions, which facilitates control of each section by respective organizational branches. Thus, everyday activities of the forces are controlled by staffs using various traditional means of communications, usually equipped with encrypting equipment of guaranteed or temporary reliability: telephone, telegraph, encrypted communications, couriers, etc.

The condition and employment of nuclear weapons are monitored with special systems and means of combat command and control (for instance, *Signal* in SRF), which have absolute priority over all other means of command and control. There are also divisions of responsibilities within the combat command and control systems.

Routine control of nuclear weapons' technical condition is carried out via separate tracks of the automated combat control system all the way down the chain of command posts. Technical information from the lower levels of the command and control system is generalized and analyzed by the main directorates for operation and maintenance of nuclear weapons. All problems and accidents involving nuclear weapons are immediately solved and analyzed, resulting in the appropriate subsequent technological improvements.

Finally, the main responsibility for combat employment of nuclear weapons falls within the competence of the nuclear forces' operational personnel: combat duty crews of command posts and staffs at all levels, particularly the operations departments and communications personnel. The track for transmitting commands and receiving reports about execution of orders is separated by technical means from all other functions within the automated combat control system itself. The number of personnel with direct access to combat command and control is strictly limited and these limits are rigorously monitored and enforced.

2. Blair's claim that "standard practice of keeping nuclear warheads apart from their delivery units," is not directly related to C^3. It is sufficient to say that this practice is not applied to most types of Russian nuclear missiles.

3. The "two-person rule" is indeed implemented at Russia's nuclear command posts. For instance, launch operations in an SRF regiment can be conducted only by two members of the duty crew simultaneously. The control tools (buttons, keys, etc.) are located on the equipment and designed in such a way as to preclude their use by one person. They are at such a distance from one another and are synchronized in such a way that, for instance, if one person attempts to activate sequentially two "separated" control tools, the whole system automatically turns itself off. This rule also applies, although somewhat differently, to all higher level command posts, including the General Staff. But at this level, not only two operators but also a larger number of people must simultaneously "want" and be "able" to give launch orders to the forces.

One may add that all technical command and control assemblies and combat documents required for launching the missiles are kept at the command posts in specially controlled, reliable safes, equipped with alarms.

4-5. The higher command posts exercise continuous technical control over possible unauthorized actions in the subordinate sections of C^3. For instance, the SRF's *Signal* system (*Signal*-M and A) provides for an immediate, automatic, top-priority report, "NSD!" (*nesanktsionirovannye deystviya* – unauthorized action!), from the command post "at fault." up the whole chain of command, including the Central Command Post of SRF and the Central Command Post of the General Staff.

On several occasions during my service in the SRF Main Staff, I took part in emergency investigations conducted in SRF divisions to find the causes of such automatic reports, which happened infrequently from time to time. All of them were caused by technical problems in the equipment or by operators' mistakes. All these incidents were thoroughly analyzed, with consequent improvements in technology and manuals to prevent repeated mistakes. In this way, the command and control system was debugged.

These illustrations of the Russian command and control system's ability to provide automatic reports on unauthorized actions testify to its robustness. During the entire period of the SRF automated combat control system's operation, there has not been a single case of intentional unauthorized action, to find out the codes, etc. At least, I know nothing of such incidents, and it is impossible to hide information about such extraordinary events within the nuclear forces. I believe that there truly have been no such incidents because of the extremely "respectful" attitude toward nuclear weapons on the part of everybody who knows anything about them.

Technology can malfunction; there is nothing surprising about it. It is much more important to know *what* may result from these malfunctions. There are two important issues involved: first, how can such malfunctions be neutralized within the system itself, and, second, how do people behave in such a situation?

Malfunctions that took place within the Soviet/Russian C^3 were neutralized by the system's design principles. Their undesirable consequences were blocked by the algorithm of pre-launch operations, which requires that each command receives a response,

and all subsequent operations also require a response from "below." The malfunctions I know about were in the initial stages of the whole process.

As for people (first, duty crews in command posts), in peacetime they operate on the basis of common sense. In the mid-1970s, there was a case of technical malfunctioning in the SRF C^3 system from top-to-bottom. Because of a technical mistake, the troops received an automatically transmitted preliminary order to put the C^3 system on combat alert. All the duty officers in the command posts realized, up the chain of command (in SRF armies and the SRF Central Command Post), what was going on, except for one duty officer in a division command post, who started to implement the order and put his unit on alert. This level of alert is part of very preliminary procedures, and could not have any serious consequences leading to an unauthorized missile launch.

How should we evaluate the actions of duty officers? Of course, from purely military standpoint, the only "disciplined" lieutenant colonel was right. And, from this formal standpoint, he was rewarded. But from the human standpoint, everybody supported the remaining majority of duty officers: the international situation was quiet, everything was peaceful, and one could not act blindly.

It was different in times of international tension. During the Cuban missile crisis, I was on temporary duty at a rocket division located near the city of Nizhny Tagil, and I was present at the command posts when authentic orders were transmitted from Moscow to put all SRF on the highest combat alert. Orders were carried out quickly and skillfully at the command posts, but it was strangely quiet. I cannot forget the mixture of nervousness, surprise and pain on the faces of each operator, without exception – officers, enlisted men, and women telephone operators. This should never happen again.

For the sea-based nuclear forces, the questions of controlling unauthorized actions are a bit more complicated than for the SRF. Since SSBNs cannot give continuous feedback to the center, it is impossible for them to report any incidents immediately. There is no evidence of attempted unauthorized actions on board Russian SSBNs.

Most experts in Russia and in the United States are convinced that Russian SSBNs still have no capability to launch SLBMs autonomously, without sanction from the center:

> "There is definite evidence that external input information from outside the vessel was needed to enable the crew to fire its missiles. Perhaps the strongest evidence came from a former Delta-II and Delta-III class SSBN crew member, whose version of the launch procedure alleged the existence of electronic blocking systems that needed to be lifted prior to launch. Special unlock codes had to be received from higher authority and punched into the on-board weapon system computer to deactivate the blocking system that prevented unauthorized launch ... Another Soviet military source familiar with SSBN launch procedures confirmed this account but added that the procedures varied with circumstances."[188]

To be fair, one must mention that some sources express doubt in this matter. In particular, references have been made to statements by the former chief of the General Staff, Marshal Akhromeev, and former military advisor to the Ministry of Foreign Affairs, Gen. Geliy Batenin, made in private conversations with the U.S. military:

> "Akhromeev indeed told Western visitors in a private meeting that Soviet SSBNs were not equipped with blocking devices that required coded input from higher authority prior to launch. Gen. Batenin, a military adviser to the Russian Foreign Ministry, also claimed that SSBNs had physical autonomy and could technically have fired without authorization."[189]

It is difficult to determine what the actual situation is on the basis of unofficial information, without knowing the context and circumstances of these conversations. Today, the combat manuals used by the Russian Armed Forces have nothing to say about autonomous SLBM launches. According to a recent study, this has been the situation since the early 1970s.[190] Nevertheless, the very fact that there are doubts in this matter suggests that this issue is worth studying within broader discussions about C^3 problems.

Airborne SNF also have problems with continuous feedback to the center about unauthorized actions from a plane that is at a great distance. Here, the problem can be partially resolved by strict limitations on peacetime flights with nuclear weapons aboard. The problem is solved when the strategic bombers are on the ground at their permanent bases.

6. Regarding technical blocking devices, let us note again that they are installed at all levels of Russia's C^3 system, as confirmed by U.S. sources:

> "Most Russian nuclear forces – all strategic weapons and most tactical weapons – must receive unlock codes from higher authority, without which the weapons cannot physically be dispatched or detonated. The unblocking system for their ICBMs is especially sophisticated in that only those weapons designated for immediate launch need be unlocked, and after a short period they are automatically locked up again if for any reason they had not been launched as planned. The U.S. unblocking system lacks this sophistication."[191]

The values for blocking codes are prepared and stored only in the General Staff. Periodically, the General Staff, using the appropriate departments in the main staffs of the nuclear triad, renews these codes among the troops. Special blocking assemblies are set and inspected in Moscow and then delivered to their destination. In the process of exchanging old assemblies for the new ones, not a single participant knows (or can

learn) the real values for the combat codes. It is impossible to copy information from the assemblies, and if such an attempt is made, the code values are automatically erased. There is also a system for rapid replacement of compromised codes.

5.1.2 American PALs

A brief history of the creation and evolution of American blocking devices, known as PALs:

Once nuclear forces appeared in the United States, the issue of separating the *control* of nuclear weapons from their *possession* arose: "... to achieve use control by decoupling control of the weapon from possession of the weapon."[192]

In 1958, Fred Ikle (at that time with RAND Corp.) was the first to propose the idea of combination locks for nuclear weapons. Then, John Foster at Lawrence Livermore National Laboratory and Harold Agnew at Los Alamos National Laboratory refined the idea. Prototypes of electromechanical, remote-controlled combination locks were developed. Their first models were installed on gravity bombs and missiles based in Europe.

Initially, the military resisted the new concept, fearing that it would reduce the weapons' combat readiness. Some even thought that the Kennedy administration, unenthusiastic about tactical nuclear weapons (TNW), simply "locked" them. But after National Security Action Memorandum 160 in 1962, PALs began to develop. It was necessary to strengthen control and protection with a minimum negative impact on combat readiness and the ability of the operators to function. These requirements resulted in the "secure container concept."

PALs of categories A, B, D and F were used in TNW: Pershing-2, Lance and cruise missiles. These PALs used the two-man rule, by which launch required the combined actions of two operators inputting a dual code to the weapon. These locks were protected against "picking." A "limited try" rule (a limited number of attempts to break the code) was also implemented.

Nevertheless, all blocking devices of these types can, at least in theory, be penetrated, although with considerable difficulty. To avoid this, the bypass prevention method was invented. Processing of electronic information, based on cryptographic technology, was introduced into the control switches and control circuits of the nuclear weapons. In addition, other (active) protection systems included:

- sensor membranes for detection of penetration or attempted penetration;
- a long-life power supply for such sensor membranes;
- a series of changing penalty responses, which disable critical components of nuclear warheads or destroy them in case of penetration by unauthorized personnel;
- a choice of any type of penalty response.

Initially, it was a matter of protecting the nuclear warheads and missiles. But then

the two-man rule resulted in the development of launch control methods for ICBMs and SLBMs:

> "By the end of the 1970s, almost all land- and air-based U.S. tactical nuclear weapons were equipped with PALs, and all strategic bombers and missiles assigned to the Strategic Air Command were equipped with PALs or coded switch systems, or both. The Air Force rejected the use of PALs in favor of coded switch devices for the B-1 bomber in order to save money, whereas the U.S. Navy has resisted the imposition of any such device."[193]

The two-man rule required that two people of equal training and level of responsibility carried out every sensitive operation involving nuclear weapons. "No lone zones," where a single person could not be present, were delineated around nuclear weapons.

The best solution for problems of negative control was found for the Minuteman systems. Emergency message materials, codes and launch keys were located in the LCCs in such a way as to provide both for protection against accidents and high launch readiness.

At the same time, introduction of PALs complicated the operation of C^3 systems. It was necessary to decide which of the weapon systems' elements should serve as home for control and blocking devices. It was necessary to consider the possibility of relatively widely-circulated codes being compromised. Keeping different codes widely apart, physically, from one another could reduce the weapons' survivability. Nevertheless, the experts at the Department of Defense succeeded in developing a C^3 system capable of acceptably flexible code transmission as well as recall capability, if necessary, at the peak of a crisis or at the moment of its resolution. This system, with training codes as well as one real code, allowed for training without loss of control.

Strategic bombers received devices that block missile launch and release of gravity bombs until the aircraft commanding officer inputs his personal code to the bomber's coded switch system. These devices solved other problems as well: "Such systems prevent, for instance, the bomb racks from dispensing their stores or prevent the beginning of a missile's terminal countdown to launch."[194]

It was also difficult to exclude the possibility of unauthorized use if communication channels for receiving codes are disabled. Deterrence could lose some of its robustness if an aggressor decided that he could destroy these communications channels. This problem was particularly difficult for sea-based nuclear forces.

Until 1997, the U.S. Navy refused to have PALs and similar devices, and implemented a concept of its own:

> "There are no PALs or coded switch devices on the submarine ballistic missile force, or for that matter on most other naval nuclear weapons. Certain naval weapons such

> as the submarine-launched cruise missile and all antisubmarine warfare weapons have been equipped with PALs, but the protection is removed when the vessels carrying them go to sea on mission. Navy policy evidently calls for restoring PALs protection when the vessels complete their missions, return to port, and transport weapons to storage depots on land."[195]

Protection against unauthorized actions was addressed in U.S. submarines in the following way, until 1997:

> "The procedures in use in the submarine-launched ballistic missile forces (whose warheads have no PAL-type devices) are authorized through the Navy nuclear weapons surety program. Those procedures are designed to prevent unauthorized launch. The necessity to involve most of the crew of the submarine in a launch is ensured by procedures in the launch check lists. The launch control process begins with receipt of a launch message that must be announced to the entire crew. The radio message is verified by two teams of officers (not including the commanding officer, weapons officers, or navigator, all three of whom have separate functions in the chain of responsibility). Special keys are then issued to those responsible for certain specific functions (pre-launch custody of the keys is assigned to personnel not in the launch sequence), so that a series of "permission" switches can be closed in the prescribed sequence. Each member of the crew is kept informed through public address announcements and telephone dialogue. These procedures justify the confidence of the national command authorities in the integrity of the SLBM launch control system."[196]

The description above indicates that this unusually complicated launch procedure involves the whole SSBN crew along with reception of a launch command from above. At the same time, however, only two operators launch Minutemen under the same conditions. Why the difference? Many sources suggest that U.S. SSBNs could launch SLBMs without authorization.

This situation was referred to in congressional hearings in 1991:

> *Bruce Blair*: "This situation is in contrast to U.S. forces, at least those at sea, which I think most people know are not physically incapable of launching their forces without such codes. They are physically capable ..."
>
> *Sen. Joseph Biden*: "For example, as I understand it, and this is not classified information, I am just speaking from the public literature, there is on the U.S. submarine system no technical safeguard to prevent launches without authorization from a higher authority. In other words, the submarine commander who had the coopera-

> tion of certain members of his crew could launch nuclear weapons at his or her own discretion. Indeed, if he were a commander of a Trident submarine, theoretically he could launch up to 200 warheads, each of them with 10 times the destructive power of what was dropped on Hiroshima."[197]

The main reason for this peculiarity was the great probability of loss of communication between the SSBN and the center under combat conditions. This system, however, aggravated the problem of negative control in the sea-based component of the U.S. strategic forces.

In 1997, according to Blair, the U.S. Navy yielded to pressure from defense civilians to equip Trident submarines with technical seafeguards that would prevent the unauthorized launch of missiles. A special safe was installed in each boat for this purpose. Each safe has an inner safe whose unlock combination would normally be provided in a wartime launch order from higher authority. Opening the inner safe with the combination gives access to a special key to be inserted into the main fire-control console of the boat's command post. Without easy access to the key, no missiles could be fired.

This does not represent a true PAL, and this new physical barrier is not ironclad protection against unauthorized efforts to gain access to the critical launch key. But, it represents a further centralization of technical control outside the boat and a shift of priority further away from positive control and toward negative control.

5.1.3 The National Command Authority

One needs to address the issue of protection against unauthorized actions at the NCA level. One mistake there can lead to a global catastrophe.

If lower-level solutions to the problems of negative control are for the most part technical in nature, at the NCA, such problems require solutions of an organizational nature, with considerable attention to the psychological and philosophical aspects.

Theoretically, a command and control system cannot be completely protected against mistakes by those who are in charge of a nation at a critical moment. Why? First, "absolute negative control" makes impossible, as seen from the term itself, any use of nuclear weapons whatsoever. Second, even national leaders are only human. In the final analysis at the NCA level, everything depends on the integrity of the main actors.

Blair describes the actions of Russian strategic C^3 during the 1991 attempted coup: "The established technical and organizational procedures had not been able to cope with such upheaval at the apex of command and could not by themselves resist the designs of the coup leaders."[198]

Blair notes, correctly, that whatever the protective measures undertaken in advance, the effectiveness of negative control is reduced at moments of social or international upheaval: "Socio-political factors motivated these remedial actions. By the same coin, deviations from established procedures could undermine the negative function. The

effects of socio-political factors on control can cut either way. They may be beneficial or harmful, depending on the circumstances."[199]

Blair believes that the Russian command and control system, as a whole, successfully survived this trial. The main factor was the people who actually controlled the launch capability (high-ranking military officers), who did everything necessary to protect against an accidental launch.

According to Blair, the Russian system is based on the division of competence, responsibilities and rights when it comes to the preparation of three main launch orders – launch authorization, unlock codes and targeting instructions. Indications of an enemy attack would be the basis for issuing those orders. This information is, in general, similar to that quoted from another source in Chapter 4.

According to numerous assessments by American experts, Russian C^3 adjusted to the situation during the coup attempt and successfully blocked any possibility of accidental or intentional actions with nuclear weapons on behalf of the conspirators, even though there is no evidence of such attempts. The major barrier in the command and control system against mistakes and their undesirable consequences during the days of the coup attempt were the actions of the commanders in chief of the main components of the nuclear triad – SRF, Navy and Air Force. Those commanders decided, between themselves, not to carry out the conspirators' orders; to refuse assigning them the required experts, equipment and documentation; to maintain the command and control systems in manual, rather than automated, mode; to carry out a number of pre-emptive measures in their troops, which was done immediately; and also to maintain a constant exchange of information regarding the developing situation.

One can agree with this positive evaluation of the commanders in chief's actions by American sources. By no means were their actions in violation of procedure or an act of insubordination. The top generals demonstrated high responsibility and considerable political maturity by excluding opportunities for employing nuclear weapons as a dangerous ace card in a messy political game. It only remains to add that this pattern of behavior was demonstrated not only by high-ranking generals but also by all the nuclear staff and troops who carried out the pre-emptive measures in a clear and conscious way.

The U.S. military have demonstrated a similar behavior pattern during acute moments in the country's domestic political life: "During the final days of the Nixon administration, the kind of implicit veto that can occur was applied when Secretary of Defense James Schlesinger instructed the commanders of U.S. forces not to obey any unusual order from the White House without confirmation from the Pentagon."[200]

Blair describes alternative opportunities to exercise negative control beyond what the Russian C^3 system demonstrated during the coup attempt.[201] Most of them actually exist.

Thus, Gorbachev's "nuclear briefcase" could not be used, even though the conspirators confiscated it and sent it to Moscow. On board the plane, the officer responsible for its safekeeping allegedly erased all the information contained in it. There is also a

theory that the suitcase had been rendered unusable even earlier – at the Foros country house when it had been disconnected from all external communication channels. At the same time, after the president's nuclear briefcase "disappeared from view," operators of a special control system in Moscow deactivated two other briefcases according to an established algorithm. Those were in the possession of Marshal Dmitri Yazov, the defense minister, and Chief of the General Staff Gen. Mikhail Moiseev (the former had participated in the conspiracy; the latter was "in the shadow"). Just in case, the military decided not to allow Gennady Yanayev, pretender to the job of head of state, access to the special communication system *Kazbek* mentioned in Chapter 4, thus excluding him from the "game." Some other similar measures are mentioned.

This picture may or may not be quite correct and true in specific details, but it is clear that such measures should and do exist in Russia's C^3 system. It is very bad, however, that nothing is known for sure about those safety measures. This means that we cannot correctly assess their reliability, initiate effective efforts for eliminating dangerous flaws and improve the system further. Thus, lack of knowledge about negative control is its main problem.

The second controversial aspect that American authors pay attention to is the possibility that the military might act independently, without presidential authorization. If many aspects of the Russian negative control system are unclear, this factual break in the command and control chain between the political leadership and the military is an obvious fact: "If communications with both the president and defense minister are severed, the Chief of the General Staff acting alone could authorize retaliation by various means, including the Dead Hand system."[202]

Generally speaking, the situation is the same in the U.S. strategic forces. When Col. Gen. Igor Sergeyev, the SRF commander in chief, visited the United States in 1993 and asked duty officers at STRATCOM whether they could launch missiles without presidential authorization, they, after some embarrassment, responded positively.

Is this good or bad? With all the challenges of providing a straightforward answer, it seems that this general principle is rather more good than bad. It is probably more reliable to take the key from the monster's cave and give it to a large group of people who are technically sophisticated, understand nuclear weapons, and their command and control, and endowed with the highest sense of responsibility due to their knowledge of a nuclear catastrophe's consequences. One person, probably not less responsible but certainly less competent technologically, may commit a tragic error in a moment of stress (or with evil intent in some exceptional case). This conclusion is, to a certain degree, confirmed by the behavior of the Soviet C^3 system during the days of the coup attempt.

The third "negative aspect of negative control" is rigid centralization of the Russian command and control. American sources state that, for all mid-level and lower units of the chain, any order from above will be considered legitimate – no matter who issues it and with what purpose.[203] They emphasize that the lower levels of C^3 are practically

unable to do anything. According to American experts, the U.S. C³ system is less centralized and therefore better. My argument is that in both cases only the degree of centralization – that is, what level has the right to issue launch orders – is different. In the long run, executing units are in more or less the same position in both countries.

In the next section, we will discuss in greater detail the question of delegating nuclear responsibilities. Here, it is necessary only to state that, from the point of view of negative control, it is better to have a more rigidly centralized chain where the very top of the chain is reliably protected. A case in which lack of confidence in the leaders is compensated by delegating responsibilities to a whole series of command levels, one of which may prove unreliable, seems to be a less sound one.

A general problem for any nuclear state is that at the very top echelons of C³, organizational, not technical, measures prevail. And even though such a situation cannot be completely changed, there should be an effort to introduce greater implementation of reliable technical systems and safety measures at the very top of the system.

Summarizing the discussion on negative control, it is evident that there is considerable similarity between both sides regarding the problems that exist in all the areas of ideology, organization and technology. This is not surprising since the final goal of all measures is identical for all parties. Those problems will not be resolved in any normal way without a mutual exchange of information between nuclear states. Not only information but also cooperation and mutual aid are crucial.

During Senate hearings in 1991, Biden expressed a wish to change to practical cooperation by suggesting the formation of a special commission consisting of Soviet and American C³ experts. This met with the approval of everyone present:

> "The commission would consist of civilian and military experts from each side. Experts such as our witnesses today, who should begin meeting with each other as you two have, first to share information that would lead to stronger protections on each side against unauthorized or accidental use of nuclear weapons. And second, to share ideas and develop joint recommendations as to how the two sides can achieve early and massive reductions in their nuclear arsenals through simultaneous measures."[204]

But such a commission was never created.

Avoidance of unauthorized actions with nuclear weapons should become the main point on the agenda of all nuclear states, not just as a figure of speech but as an existing practice. The limit of such efforts is in reality impossible to define. Negative control requires much less financial expense than positive control, and is much more meaningful today. Blair notes: "The Soviet command and control system was deeply fearful of a breakdown that could lead to the illicit use of nuclear weapons. Its obsession led to the imposition of tight central control and elaborate safeguards."[205]

It is possible that such "obsession" could be useful now on both sides.

5.2 C^3 Survivability: Is There a Solution?

Along with negative control, one of the main problems for strategic C^3 systems is their survivability under combat conditions. Notably, if survivability requirements are satisfied, the goal of expected positive control reliability has been achieved.

Command and control survivability is the characteristic of positive control that has the most influence on its effectiveness. If, indeed, we take as an indicator the system's speed of operation – its technical ability to perform certain actions with a given speed (first and foremost, launching the missiles) – there are no serious problems in this area at the present time. Modern command and control means resolve this problem as a whole by employing computer technology and high-speed communication channels.

Another indicator, secrecy, is also not crucial. First, the methods for encrypting information with guaranteed security are widely used in command and control systems in peacetime. Second, with the beginning of combat, secrecy considerations are no longer important – especially in the first stage of the conflict (if we assume that there will even be subsequent stages). In general, it is possible to issue a launch order openly, which happens in some scenarios of command and control systems employment.

Flexibility of operational use – the command and control system having necessary plans and scenarios, and the ability to change them quickly – is also present, as was discussed earlier.

Lastly, one more important requirement is reliability (accuracy) of information. Opportunities for distorting information passed along the channels of military command and control (preliminary and executive launch orders, reports up the chain of command, etc.) are not great even under an enemy's countermeasures. This is achieved with the help of reliable modern methods for increasing the reliability of communications – interference-hardened coding, numerous repetitions, reversed checks, etc. The only global problem remaining in the reliability of command and control systems is confidence in information from the technical EWS. With all due respect to the efforts of scientists and engineers in this area, even the achievement of "perfect" EWS reliability may be considered theoretically unachievable. The analysis of this problem, however, is outside the scope of this work.

Thus, survivability of command and control systems remains the most serious problem directly related to the effectiveness of positive control:

> "Despite considerable progress made in hardening and adding redundancy to U.S. command and control, one of the most significant dangers of nuclear war remains the possibility that in a deep crisis or conventional war a precursor nuclear 'decapitation' strike, perhaps by Soviet closely based submarines, against central U.S. command and control targets, might appear to be the least disastrous military option available to the Soviet leadership."[206]

Expressed in 1989 by a leading American expert, speaking about the then "probable opponent," this concern remains a valid argument in the planning of American C^3, in spite of crucial changes in the relationship between the two nuclear superpowers. Of course, a parallel argument is also used, in this or that form, in Russia. Efforts are made by both sides to improve the survivability of C^3.

Let us briefly review American assessments of U.S. and Russian C^3 survivability:

5.2.1 American C^3

One of the sources analyzing the nuclear threat to American command and control systems is a study by Pry.[207] In *C^3I Survival* the following potential goals of attacking the systems are listed:

- degrading the American ability to retaliate;
- decapitation of U.S. nuclear forces and their isolation from the military leadership;
- reducing effectiveness of air defenses, to facilitate bombers and cruise missiles entering American air space;
- degrading American ability to conduct a protracted nuclear war;
- "severance of connectivity between the NCA and the strategic forces [that] could deny the United States the capability to employ its forces, or to employ them in a strategically and politically sensible way."[208]

For convenience's sake, we will substitute what Pry calls the "Soviet side" with "opponent."

In Pry's opinion, the opponent is capable of conducting a limited nuclear attack several minutes prior to a massive nuclear strike. The goals of such an attack would be to deprive the United States of its ability to detect the subsequent main strike or conduct a retaliatory strike. An alternative scenario is to use a period of conventional war to weaken American defenses and its readiness to resist a sudden attack. According to the author, those preliminary attacks may have different characteristics:

- striking the EWS;
- attack employing EMP weapons;
- attack against command and control posts and against LCCs;
- physical destruction of the country's leadership;
- a series of sabotage operations against the main elements of C^3.

Destruction of radars and ground support complexes for ballistic missiles EWS and Precision Acquisition of Vehicle Entry Phased – Array Warning System satellites (five of the last six are outside of the continental United States) will leave the United States blind. The opponent's submarines are capable of doing this with cruise missiles armed

with conventional or tactical nuclear warheads. Timely detection of such an attack is a very difficult task.

Almost all parts of the American EWS are located on ocean shores, and submarines may commit acts of sabotage against them. This is also true for other C^3 elements:

> "The bombers in the Arctic rely on the Green Pine system to relay the [Emergency Action Message] to them by UHF after receiving it from Looking Glass or [Emergency Rocket Communications System]. As noted, Looking Glass has access to the stations through a simple node at Elkhorn, Nebraska, which could easily be destroyed. Even if [the Emergency Rocket Communications System] survived to deliver the [Emergency Action Message] to the Green Pine network, the network itself could be directly attacked."[209]

American experts evaluate various types of super-EMP weapons as a serious threat to the Armed Forces in general and especially to their command and control systems. According to many experts, an EMP attack is capable of "pinning" Minutemen in their silos, destroying bombers and launched missiles en route, and severing communications with the nuclear forces completely. It is thought that the entire American East Coast can be "covered" by the explosion of an EMP charge at an altitude of 500 kilometers, three minutes after launching it from a submarine in the Atlantic. There are also alternative, equally effective scenarios of EMP attack.

Americans are involved in thorough research and, wherever possible, implementation of weapons and command and control system EMP-hardening. Three main methods of such hardening have been discussed:

- computers, telephones and other communication equipment are shielded by special steel boxes known as Faraday's cages or are located deep underground;
- cable lines and antennas are isolated from electronic equipment with the help of surge arresters, i.e. devices similar to those used against lightning. (In Russia they are called "lightning arresters." Regular lightning arresters cannot be used against EMP weapons, so special ones are built with a very low level of inertness, comparable with the exceptionally short duration and steep leading edge of EMP);
- wide use of fiber optic technology, which is practically invulnerable to EMP weapons. In the last 10 to 15 years, a number of projects were under way in the United States using fiber optic technology in command and control of MX missiles and B-1 bombers.

Implementing EMP-hardening is, however, very challenging. Together with the high cost (up to 20 percent of the hardened site's general cost), there are doubts about the general effectiveness of those measures. Full-scale experiments simulating combat

conditions as closely as possible can only be carried out during nuclear weapons tests, which are currently not being undertaken by the United States. Available simulations are not reliable enough. (This is a true paradox of our times – banning nuclear weapons testing prevents developing defense mechanisms! And the most effective solution to this problem can only be elimination of the topic itself – nuclear arms.)

Pry thinks that it is also possible to carry out a strike against the LCCs of silo-based U.S. ICBMs prior to the main nuclear attack. He sees a flaw in the fact that a large number of Minutemen and MX missiles (with even more warheads on the latter) are controlled by a relatively small number of LCCs. These command posts are vulnerable to submarine attacks with conventional and low-yield nuclear charges. Sabotage is also possible. ALCCs may prove unreliable. There is only one ALCC per each wing of SAC. They may be incapacitated while still on the ground or in the air by EMP weapons. Communications between ALCCs and the missiles may be disrupted due to high altitude nuclear explosions upsetting the ionosphere, etc. ALCCs cannot stay within the SAC wings' line of sight for a long time; they have to land periodically at their own bases which may themselves be destroyed.

The author also does not exclude the possibility of decapitation of the U.S. nuclear forces as a result of the assassination of political and military leaders, along with wide-ranging sabotage against crucial elements of the command and control systems. Here he cites as an argument the considerable attention paid in the Soviet Union to perfecting the Spetsnaz forces. According to his data, there were between 12,000 and 30,000 Spetsnaz troops as of 1990. He also mentions the "formidable experience in the U.S.S.R." of jamming Western radio stations (*Voice of America* and others). This experience and still existing equipment may, as mentioned in the book, be effectively used, especially prior to a nuclear attack.

There is no need to recount all the dramatic scenarios of timely penetration into U.S. territory by Russian saboteurs with atomic demolition munitions. Even more "dramatic" things were gamed during nuclear exercises on both sides over the last 30 odd years. Today, nothing seems unrealistic in a world shaken by acts of international terrorism. Here, we are, of course, talking not about plans by Moscow or Washington, but about the existing potential of serious provocations from "third parties." Therefore, Pry's concern about timely prevention of such actions against C³I is easily understandable today.

There are other sources worth mentioning here that consider potential threats to American command and control systems. Let's quote from one of them:

> "Conventional conflict also threatens the following U.S. strategic control elements deployed abroad: low-frequency and very low-frequency radio towers for SSBN communications, SAC high-frequency radio towers for strategic aircraft communications, overseas bomber recovery bases, bomber strike assessment relay stations,

> and SSBN port facilities and tenders. ... Many other satellite constellations support strategic and non-strategic units: meteorological, navigational, signals, intelligence, and communications. Electronic and physical attack on them during conventional war would degrade U.S. strategic nuclear capabilities as well as conventional capabilities. ... Major command and communication nodes in air are also largely fixed and vulnerable. The lack of modern, protected command posts and communications is widely seen as the greatest deficiency in the theater nuclear area."[210]

Blair also points out the relatively low survivability of American C^3. He notes that even collateral damage to C^3 elements from attacks on nuclear forces themselves can disrupt command and control:

> "A Soviet attack designed to inflict maximum damage on U.S. nuclear forces the possibility that underlies the principal perceived weakness of U.S. deterrence – would coincidentally produce extensive damage to the U.S. command structure. Many C^3I elements would come under direct attack because of physical proximity to SAC bomber, tanker, and Minuteman bases."[211]

Further on, the author lists direct threats to command and control coinciding with those mentioned earlier.

I would like to end this rather gloomy description on a more cheerful note. Here is a quote from a "salty admiral," also relevant to the problem of C^3I survivability (it was noted earlier that each submarine tows a long antenna): "I have looked through my periscope on the USS *Will Rogers* and have been horrified to find there are birds roosting on the doggoned wire back here ..."[212]

As for my comment on the material discussed in this section, I have only one: True, all those threats to command and control systems are theoretically possible. Yet their practical implementation does not seem that easy when looking at it from the other side. Nor does the American C^3 seem from that other side to be so vulnerable.

5.2.2 Russian C^3

American experts' views of Russian C^3 survivability problems are considered here on the basis of Blair's work, which analyzes its hypothetical combat stability on two levels: high-level strategic command and low-level command posts.

Blair is somewhat harsh with the Russian C^3, having decided that it is vulnerable on both levels. He describes the highest level of this system as nuclear Netherlands because of a "huge labyrinth of underground bunkers." According to his data, in Moscow and its suburbs alone there are about 75 deep underground structures with protection of no less than several thousand psi.

Despite the existence of a well developed network of highly protected stationary structures all over the country – according to some estimates there are 2,000 to 2,500 of them – and permanent representation of the central authority on the periphery, the old Russian habit of "maximal centralization" makes sure that all the command and control in the armed, and especially nuclear, forces are concentrated in a few key bunkers in the Moscow area. The most important ones are mentioned in Blair's book, being discussed here. The author believes that the biggest one is a structure in Ramenki that can house up to 10,000 people and is 650 to 1,000 feet deep.

The CIA's 1978 study of protection for the Soviet high-level strategic command's underground command posts concluded that "all fixed leadership shelters which have been identified are vulnerable to direct attack."[213]

But already in the 1980s, using new calculation formulas, American experts concluded that more effective weapons were required to guarantee complete destruction of these bunkers. One cannot but be impressed by the thoroughness of these calculations, which take into account the peculiarities of the structures themselves, characteristics of missiles, nuclear charges, the soils, etc. If according to the old calculations the diameter of the crater from a 1-megaton charge would be 651 feet, according to the new formula it would be "only" 394 feet. This was not enough for destruction of the bunkers, according to the Pentagon experts. In the most typical locations of Soviet command posts – wet soft rock – only structures no deeper than 344 feet could be destroyed. Ultimately, the United States arrived at the conclusion that it would be difficult to incapacitate the top level of the opponent's nuclear command and control.

At the same time, Moscow continued using old formulas – on purpose, according to Blair. According to the formulas, the threat to the central strategic command posts was a "lethal" one. Soviet experts did not even exclude the possibility of employment of gravity bombs with very high explosive yields against the bunkers. They assumed that in the course of conventional war, American bombers could unexpectedly fly from Europe to Russia and strike with these bombs. Such warheads could, according to their calculations, destroy structures down to 1,889 feet deep.

This discrepancy between the results of calculations by the two sides is typical for all estimates of C^3 component survivability. And this is no small "fork" between optimistic and pessimistic assessments. This is quite natural because, first, the basic data is fully classified, and, second, the price of an error is exceedingly high. And, as Blair justly notes, "No model had been verified experimentally and proved accurate."[214]

Blair then notes that the cable communication channels and antennas coming from the command post structures are much more vulnerable than the structures themselves. He lists the already familiar factors influencing C^3 components – direct physical destruction, active jamming, disturbance of the ionosphere due to nuclear explosions, EMP, etc. Most of the radio and satellite communication lines, including their locations, can be detected by foreign intelligence even in peacetime. This argument, however, contains a small technical inaccuracy. Blair believes that antennae transmitting

fields do not provide accurate information on the location of command posts because both the fields and the radio transmitters are, for the sake of secrecy, moved a considerable distance away from the posts and are remote controlled through underground cables. This is only partially true because the main purpose of such a step everywhere, not just in Russia, is to avoid jamming one's own equipment at the command posts by radio transmitters. Despite the vulnerability "in principle" of radio communications, Blair treats the issue with caution: "It was unlikely, however, that all communications from a surviving bunker would have been permanently suppressed."[215]

Blair also analyzes the center's backup and auxiliary command and control posts, including mobile command posts with various types of basing. The key role belongs to airborne command posts. The author criticizes them harshly for their outdated fleet, "hibernation" routine in peacetime, insufficient crew training, use of regular civilian airports, etc.: "As a rule, virtually all the mobile backup components of the Soviet nuclear command and control system were kept on a low level of alert and required many hours to get ready. In consequence they were vulnerable to destruction in a surprise attack."[216]

Flaws in these elements of Russia's command and control system, also typical to a considerable degree of their equivalents in the United States, cannot be denied; yet, it would be wrong to conclude that they are totally vulnerable and lack combat readiness. Whenever possible, they are being improved, crews are being trained, and they do make a certain contribution to the reliability of the whole system.

Blair, along with his own negative assessment, refers to the opinion of the majority of American experts on the survivability of the top levels of Soviet C^3: "The uncertainties were a source of major Soviet discomfort. The flip side of this uncertainty should also be acknowledged, however. In 1990, U.S. planners had reasonable doubts they could inflict decisive damage to Soviet fixed or relocatable command targets."[217]

Lower levels of SRF command and control are also severely criticized by Blair, who thinks that in 1990, if a few dozen American missiles launched an attack specifically against the standard command posts of the silo-based ICBM regiments, they would have been able to neutralize the main part of the Soviet ICBMs.

With considerable knowledge, the author lists all the additional types of command and control at this level – mobile ground and helicopter division command posts, "redundant" cable networks within deployment areas, employment of communication systems of other services and institutions, etc. He draws the conclusion, however, that the system as a whole is vulnerable. His idea is that the basis of command and control at this level are the regimental UKP (*unifitsirovannyy komandnyy punkt* – standard command post), the equivalent of American LCCs: "If that is so, then the United States projected a potent threat to the Soviet ICBM force because it could have destroyed the vast majority of the launch control centers (LCCs)."[218]

He believes that despite the high level of UKP protection – about 6,000 psi – two MX ICBM and D-5 SLBM warheads could incapacitate each of them.

A three-stage scenario of nuclear war is described as optimal.

Stage One – an attack on all of the UKPs (LCCs). It would take only 222 nuclear warheads to deprive up to 80 percent of Soviet missiles of their main communications with the center through the UKPs. If the effectiveness of the strike is calculated, as it is often done, according to the proportion of used (friendly) and neutralized (the opponent's) warheads, it is a very alluring 1-to-23 (!).

Stage Two – an almost immediate attack against the silos themselves. Here this proportion is 1-to-2 in favor of the United States. Put together, the proportion becomes even more dramatic for both stages: 1-28 – since some of the surviving UKPs will no longer have most of their missiles.

Stage Three – "finishing off" the surviving UKPs and missiles with strategic bombers within 10 hours after the first two stages. It is thought that their command and control cannot be restored during that time.

One tends to be too overwhelmed by such a scenario to argue against it, but here I will try.

First, unlike the American LCCs, the crew of one UKP can launch (by radio) all the missiles in a division. This is always checked during exercises. Second, the author mentions *Perimetr* only in passing. Yet, within 40 minutes at the most, it will be able to launch all the remaining ICBMs. Third, the system of autonomous launches performed by special crews directly from the ICBM silos will be activated. Any surviving missile division mobile command posts will also be used. There are other launching alternatives; it makes no sense to list all of them here. And, finally, Blair reviews only the LUA scenario, even though it probably will not take place, and we will have to deal with a LOW scenario.

Thus, it is impossible to consider the case of Russian ICBM command and control as so hopeless.

Having drawn his conclusion about the unreliability of the Soviet stationary missiles' command and control systems, Blair analyses the potential of communications with mobile ICBMs. He notes their important role if they are deployed to the field in good time, and justly points to certain difficulties in communicating with them when they are deployed. Further, he stresses the high launch readiness of these ICBMs when at their permanent bases using the *Krona* systems. Blair also describes possible methods of command and control for rail-mobile ICBMs.

A few words regarding the American evaluation of the Soviet SSBN command and control systems: Blair thinks that a low degree of SSBN readiness – few boats are on combat patrol in peacetime – can be explained by the desire to maintain stable communications with them as well as rigid centralized control from Moscow. When submerged on patrol in the remote waters of the Northern Atlantic and by Greenland's shores, they continuously receive ELF control signals from the Kola Peninsula. Whenever this signal disappears, as well as when reception is good, SSBNs surface twice a day, every day, for two-way communication with the center, mostly by short-wave radio or satellite channels. American experts feel that even though this compromises stealth,

the Soviets consciously maintained this patrolling system, sacrificing survivability in the name of negative control:

> "Soviet commentators frequently voiced their concern that the United States, by virtue of dispensing with unlock devices on nuclear weapons at sea, had tipped the balance too far in the direction of positive control at the expense of safeguards. The Soviets took the opposite tack and imposed strict central control over SSBNs, an approach that created additional burdens on their system of positive release."[219]

The described system of regular communication sessions that reveal submarines' locations does increase their vulnerability. Russian boats cannot launch without orders from above, which, according to Blair, creates a series of problems in their employment. In particular, the military leadership may in some cases consciously delay issuing an order to a submarine, for fear of mistaken actions by the submarine after communications disappear. But such a delay can result in the submarine not receiving the order when the time comes.

In light of such a cautious approach, U.S. specialists view the stability of SSBN command and control as reasonably high. Blair states that near native shores, communication with submarines is also maintained, on top of all by the methods listed above, through buoys, acoustical devices, surface ships, escorting non-missile submarines and even underwater cables. From the continental shelf, the submarines periodically raise their slightly detectable antennae and receive orders. He mentions the following statement by the former Navy commander in chief, Adm. Sergei Gorshkov:

> "This very important moment of submarine control can require many complex measures and actions aimed at improving reliability of the signal's passage: accelerated launch of additional communication satellites; deployment of additional control and relay devices at sea, beneath the water, and in the air; deployment of command ships; involvement of civil radio communications centers; and reduction of time intervals for submarine to rise near the surface for radio communications."[220]

Blair concludes that several, if not any single one, of those measures can provide survivability for the command and control of SSBNs in case of a direct attack. He feels that this factor is a powerful deterrent influence upon U.S. decision-makers, while it is not enough to completely reassure Soviet experts.

The latter opinion is absolutely correct. Moscow's military leadership is seriously concerned about the insufficient reliability of command and control for the sea-based component of SNF, which considerably limits its operational employment.

Blair's general conclusion regarding the survivability of U.S. and Soviet nuclear com-

mand and control systems at the end of 1990 is pessimistic: "Command and control systems remained vulnerable despite huge investments to protect them. In the U.S. and Soviet cases their functions could have been severely disrupted by the effects of a few hundred weapons at most."[221]

This is true to some degree. The next thought of my American colleague – that this circumstance pushes both sides to embrace the LOW posture – is also correct. But, of course, this is not the best solution, and naturally the author arrives at the conclusion that a major reduction of nuclear forces readiness is necessary – global zero alert.

This is a good measure but it does not resolve the whole problem.

Let us review again the quoted American assessments of both Russian and U.S. C^3 systems. They are both "weak," but at the same time trying to decapitate them is too risky. With all their ambivalence, these assessments are logical. It only remains to determine how much command and control systems contribute to nuclear deterrence.

I'll also mention another relatively new, but very serious, danger threatening the C^3 systems of nuclear powers – "computer warfare" – that gives the fourth "C" to C^4I.

This is a very specialized, complex form of hidden military competition, which nevertheless is susceptible to certain countermeasures. Russian military computer scientists have paid attention to a certain lag in this area behind the West:

> "The leading nations have long ago recognized the danger of using unverified software in their automated command and control systems. In the United States, the Pentagon ordered the ADA system to develop software for the armed forces. In France, the programming language LTR-3 has been in development since 1986. Substantial allocations for such work are justified by obtaining reliable software protection for military systems against viruses, logic bombs, etc. ... Because new information technologies are being rapidly introduced into the work of command and control organizations in the U.S. military, a new special agency (The Defense Information System Agency) was created; it supervises software development and computer acquisitions. The Center for Computer Security has functioned in the Pentagon since 1981. Military theorists are discussing various aspects of using non-lethal software-information weapons in military conflicts."[222]

One should think that Russian leadership is taking necessary steps in this direction as well.

Let us get back to the question in the title of this section: Survivability of C^3. Is there a solution? – Possibly, there is no solution if we strive for total, 100 percent survivability. But there *is* a solution if we are able to come up with a minimal quantitative level necessary to provide for reliable mutual deterrence. This has to be done with close reference to the capabilities of nuclear weapons themselves.

As shown in this section, threats to C^3 are of such a nature that protecting C^3 is very

difficult and very costly. Limiting development and testing of new types of anti-C^3 capabilities is necessary but cannot be a panacea, because attempting to stop or even slow technical progress is impossible. This competition between offense and defense can continue indefinitely, with unjustified spending and periodic crises in strategic stability.

Evidently, the resolution to this problem lies in a different area. We need to prove the existence of a limit that cannot be overcome by any technical advantage of one side without the risk of punishment for the attempt to use such an advantage. It is a mechanism similar to the idea of "springs" presented in Chapter 3. If this goal is achieved, technical progress, including development of new means of attack, will continue at a natural pace without artificial acceleration, which would no longer make any sense. That should provide solid strategic stability.

5.3 Detargeting, Combat Readiness and Strategic Postures

The agreement between former presidents Bill Clinton and Boris Yeltsin about detargeting of strategic missiles was one of the first attempts to strengthen nuclear security by means of command and control. Without diminishing the political significance of this initiative, we should note its particular internal contradictions.

On the one hand, detargeting of missiles attempts to reduce the danger of accidental or unauthorized launch; that is, to increase the effectiveness of negative control. This is the main aspect of detargeting.

The second goal of this initiative is to reduce mutual fear of an enemy's surprise attack. Implementation of this or that detargeting scenario should, in principle, increase the time for bringing missiles to full launch readiness. Today, this time is about two to three minutes even for ICBMs; depending on the detargeting scenario it will increase to dozens of minutes, hours or even days. Yet, without diminishing the positive significance of this time buffer, one has to consider the potential temptation for one side to beat its opponent by urgently regenerating combat readiness in a crisis.

The paradox is that because of this peculiarity of detargeting, today's "hair trigger" situation looks the most logical and reliable. The deeper the reductions in combat readiness (from the point of view of the time it would take to get back to it), the harder it becomes to provide for the requirements of positive control.

The problem of reducing the combat readiness of strategic forces is directly related to the concepts of their hypothetical use. Today's official sources and academic studies use the following classification of potential response scenarios by the attacked side: LOW and LUA, as well DSS (delayed second strike). The difference between LUA and DSS is that, in the first case, the retaliatory strike is conducted as soon as possible, even while the opponent's attack is continuing, while in DSS the retaliation takes place only after the enemy's attack is over and analysis of the situation has been conducted. Later, we will be able to see how detargeting and other measures for reducing combat readiness are correlated to the postures of strategic forces' employment.

As we have seen, in the current international situation, without any doubt, the most attention should be paid to negative control measures; that is, to finding effective measures to prevent any accidents with nuclear weapons. It is, however, also evident that within the broad context of strategic stability such measures should be implemented without upsetting a reasonable balance between the diametrically opposite requirements of negative and positive control.

Unfortunately, there are no official unclassified sources on the substance of military and technical detargeting variants implemented in Russia and the United States. Only very brief and general statements are available, such as:

> "Col. Gen. Igor Sergeev, commander in chief of the Strategic Rocket Forces, stated on May 30, 1994 (completed implementation of the Jan. 14, 1994 agreement to detarget all strategic missiles): 'Russian missiles will not lift off in case of accidental launch because target coordinates have been removed from the missiles' guidance computers.'"[223]

American political and military leaders have made similar statements.

Some publications on detargeting that have appeared in the last several years (primarily Blair's *Global Zero Alert for Nuclear Forces*, published in 1995) were used in this section. Practically all the scenarios reviewed below are taken from this source; each of them is accompanied by the "Russian side's commentary," for the most part hypothetical. Let us not forget that Blair analyzes the potential of Russian command and control systems, when it comes to detargeting, based only on open information about C³ in the United States, fairly assuming that: "The two systems, however, are probably similar enough that the U.S. system can illustrate the detargeting possibilities on both sides."[224]

There are several potential technical variants of strategic missile detargeting. Combat watch with *"zero" flight mission* is one of them.

Russia has declared that this variant has actually been implemented for its strategic missiles in accordance with the presidential agreement. According to the official statement, all Russian ICBMs have been on duty with "zero" flight mission since May 30, 1994.

Each computer aboard Russian ICBMs, both silo-based and mobile, contains several flight missions. One of them is considered "technological," or "zero," while all the rest are combat missions. Before implementing the mentioned agreement, all Russian ICBMs were on duty with one of the "combat" flight missions. The "zero" flight mission was only used during periodic technical inspections. When on duty with the combat flight mission, receiving a real launch order from General Staff command and control channels meant automatic launch of each missile toward a specific target established for it by the main (active) SNF combat employment plan. This automatic launch of a missile was possible if it had been brought to the highest stage of combat readiness earlier.

In case it became necessary to launch a missile toward a different target, established by a flight mission also stored in the on-board computer, the number of the new combat plan would have to be included in the launch order. Any of those alternatives required no longer than 10 to 15 seconds for reverse (combat) retargeting of all the missiles.

Now, with the "zero" flight mission scenario implemented, all listed technical possibilities for retargeting have been preserved. Thus, the level of positive control – or, in other words, combat readiness of the Russian SRF – has not in fact been reduced.

Detargeting is a very small addition to the existing reliable system of negative control. Due to such powerful protection, the probability of any accidental launch is very small. The chance of giving a false launch order with a combat flight mission to an ICBM is also extremely small and comparable to the probability of a false signal that could switch the missile from a zero to a combat flight mission.

During the Cold War, both the Soviet Union and the United States chose LOW to be the main posture for ICBM employment. Within this framework, both sides were waging a virtual war for seconds trying to beat each other "to the punch" in a future conflict.

It is, however, doubtful that these few seconds could play a major role in providing for LOW. At least, it did not work for the Soviet Union when American Pershings were deployed in Germany. This fact may have influenced the Soviet leadership's decision to eliminate the newest SS-20 missiles.

It is clear that detargeting with a "zero" flight mission has more of a political rather than a military/strategic meaning. Today, mutual targeting still exists for all practical purposes. Neither side can check what combat flight missions are – or are not – stored in the opposing side's ICBM computers. Retargeting to combat flight missions from the "zero" missions may be performed extremely quickly, upon one order from the General Staff. The American side probably has the same or equivalent retargeting ability. Thus, at least from the technological and operational points of view, both nuclear superpowers are able to keep their command and control systems at the "hair trigger" level. A number of sources confirm the symbolic character of detargeting.[225]

Should an accidental or unauthorized launch happen despite all the reliable safety measures, the missile will start toward one of the planned targets (identified as the "main" one in each list of targets aboard a missile). Switching from a "zero" to a "combat" flight mission will occur automatically when the launch begins, because the missile cannot fly "nowhere." The probability of such a launch order appearing by error will not depend upon keeping the missile on duty with a "zero" flight.

To avoid an accidental strike against the "programmed," or any other, target, a different scenario of detargeting – the so-called *"oceanic lightning rod"* – may be used. In this case every missile should be targeted in peacetime at a non-American/non-Russian main target that can be purely nominal, such as a point in the ocean. STRATCOM and the Russian General Staff may easily and responsibly carry out this main targets reprogramming.

Two questions need to be addressed. First, what is the difference between the Russian and the U.S. on-board ICBM computers regarding the technical (computer) time needed to switch from a nominal flight mission to combat one, especially when there is a considerable distance between the two, such as one target being in an ocean and the other on a continent? And second, which levels of command and control will participate, during a crisis, in issuing orders to reverse the mission back to a combat target? This question is important because of the contribution that higher and intermediate level command posts make to the overall time period for retargeting.

There is no official data on the first question, either for Russian or for American missiles. It is possible that retargeting Russian missiles from "oceanic" targets to "combat" ones will take just as much time as in the "zero" flight mission scenario. As for the second question, it is not crucial: the time required to transmit the order (no more than one minute) is much shorter than the time period for retargeting. For both sides, general retargeting time will be mostly defined by the missiles' computer time.

If one side's response time differs from that of the other even by a few minutes, then the side which is "late" will find itself, for all practical purposes, in a state of a DSS. Therefore, it is important to know how the command and control system will be able to provide for retargeting and launching of missiles under such conditions.

The probability that an order will be transmitted from the top depends on the availability of invulnerable reserve elements in the command and control system, such as the Emergency Rocket Communications System *Perimetr*. As mentioned, an advantage of the Russian version of the system is its ability to transmit the order "aim and launch" (as a single order) from the General Staff to the ICBM launchers immediately, bypassing all intermediate and lower command centers. If the Russian missiles, surviving an enemy strike, receive such an order, they will be automatically targeted and launched.

In the Minuteman system, orders for retargeting and launching are transmitted not directly to the missile launcher, but via LCCs. This would have a negative effect on the massiveness of the American retaliatory strike since a part of the total number of LCCs may be destroyed in a Russian attack. This is why, in certain proposed American detargeting variants, the timely issuing by LCCs of an order to the missiles for combat retargeting is not excluded in a crisis situation. Such a proposal, however, seems questionable because of its somewhat provocative character.

The main conclusion regarding the "oceanic lightning rod" is that when it is used, the danger of destruction is reduced for real targets in case of an accidental launch. At the same time, the sides will be a step closer to a posture of LUA, since the alternative becomes more and more problematic due to increased time needed for retargeting. Apparently, there is no need to fear abandoning the LOW posture, if, of course, opportunities for retaliation after an attack have been preserved. The "pure" LOW posture is not stable and is dangerous because the national leadership can never be 100 percent sure that their decision to start a nuclear counterattack is justified by a real nuclear attack, and not by an error or a breakdown of the warning systems.

Other, more radical changes in the command and control system may provide for *erasing all flight missions from computer memories*, except nominal, oceanic ones. This makes ICBMs incapable of authorized automatic retargeting, and now the higher levels of command and control must participate in the technical chain of the retargeting process. Depending on the levels of those posts in the structure of command and control – a regiment in Russia, (or U.S. LCC), or a division in Russia (a U.S. squadron), or an army in Russia (wing in the United States) – the depth of reduction in combat readiness changes, which means that the time (hours, days) needed to get back to combat readiness can change, too.

There are two crucial questions here: the speed of restoring complete combat readiness, and the survivability of participating links in the command and control system. The difference between Russian and American potentials here, which is greater than in the "zero" flight mission scenario, makes this version of detargeting more controversial. This is explained by historical peculiarities in the principles of the systems' architecture; it is practically impossible to rebuild these systems anew and make them essentially similar.

The differences between the times for bringing the missiles back to combat readiness will be measured by hours and days, depending on the degree of reduction in combat readiness. In this case, it is probably less important to determine the concrete retargeting time periods for both sides than to analyze, in principle, the possible consequences of the unavoidable differences measured in such large absolute values.

First of all, as mentioned, the very fact of a greater difference in the response time leads to a growing temptation to get ahead of the opponent in regenerating forces during a crisis. Besides, the survivability of participating elements in command and control systems is very important here. Indeed, a long period of time needed to re-establish the SNF combat readiness (hours or days) may provoke one of the parties, under certain conditions, to conduct a quick strike by conventional or nuclear weapons against key command and control points, where the opponent's technical retargeting capability is stored. When all flight paths have been removed from ICBMs and are stored at regimental and divisional command posts, the number of such key points becomes substantially smaller than in the cases of detargeting implemented directly in all launchers (i.e., "zero" flight path or "oceanic" flight path).

In this context, Russia's security will be less robust than that of the United States. First, in the American system, the remote introduction of new scenarios for the missiles by the launch command posts is done more quickly than in Russia. Second, U.S. command posts are less vulnerable to conventional weapons than their equivalents on Russian territory. Third, the "insurance" role of the Russian *Perimetr* subsystem would be negated in this case, in as much as this system is only capable of transmitting the short order to target and launch, not to install a detailed target program proper into the memory of the ICBM on-board computer. Finally, one must remember the asymmetry of the U.S. and Russian nuclear forces basing. There are many more land-based ICBMs in

the Russian strategic forces than in the United States, where SSBNs play the major role.

Some analysts suggest that the effectiveness of the latter variant be increased by organizing permanent, ongoing, *mutual on-site inspections* to check for fulfillment of a detargeting agreement. This idea has the right to exist, even though it is quite evident that, from purely technical point of view, detargeting control is extremely difficult. But in the long term, technical details are not that important; the whole issue can, morally and ethically, be seen in light of the well-known problem of hostage taking. These inspections cannot become a reliable tool to protect against the inspected side urgently retargeting its missiles for combat missions. Nevertheless, the goal of monitoring and control is crucial in any detargeting scenario.

In this regard, it makes sense to study the proposal for cooperative development of a unified automated system of operation and control for Russian and American nuclear weapons. Certain preliminary sketches for this system have already been worked out by the Impuls Corp. Those preliminary studies substantiate the need and the potential for creating such a unified technical complex that would provide permanent and reliable control over the state and degree of combat readiness of the "opponent's" nuclear weapons, but at the same time would not limit freedom of action for either side. According to Russian experts, this system would make a major difference in preventing nuclear accidents.

It is clear that scenarios in which the missiles themselves are stripped of their ability to retarget, and this ability is transferred to command posts, take both sides further away from the LOW posture. One can also propose a variant whereby parts of the targeting devices themselves are removed from the missiles and stored at the command posts of regiments, divisions, etc. In this case, missiles cannot launch at all, so protection from accidental launch is total. The important problems would be: Where will the removed devices be stored? How to combine protection and survivability of those storage structures? And how much time it will take to physically install the devices back aboard all the missiles?

In general, this approach is equivalent to other methods involving removal of any command and control device from a missile (a receiver, for example) or even a part of a missile itself (part of an engine, etc.). In this connection, the unilateral suggestion by President George H. W. Bush in October 1991 is worth mentioning: Minutemen crews enter each silo and insert a special safety pin into the engines' mechanisms. This *physically* prevents the missiles from launching. To reverse, crews re-enter the silos and remove the safety pins.

Such scenarios for detargeting strategic missiles are not fundamentally different from analogous measures with the weapons themselves (removing warheads, etc.) And it is not accidental that Blair, when reviewing all these alternatives in his book, makes a seamless transition from the detargeting problem to the essential problem of reducing the weapons' combat readiness. Detargeting and other means of reducing readiness cannot be seen as effective measures for improving strategic stability without relating

them to the broader aspects of the hypothetical employment of strategic forces.

In this connection, we need to review again, and in greater detail, the *SNF combat posture*, which is implemented through various aspects of C^3I.

Embracing a LOW strategy is dangerous and unreliabile, with its unavoidably impulsive response to EWS information, the response that can be expressed only as an immediate "launch on warning." A major uncertainty is present here, especially if we remember the rigid time limit (just a few minutes to make a decision) and skepticism regarding the feasibility of this posture, even from a purely technical point of view.

This study deals exclusively with C^3 problems, so the fourth part of nuclear command and control – "intelligence," as well as the fifth one – "computers," remain outside of its framework and are barely discussed. It does not, however, mean that they have less significance for the contribution of command and control systems to strategic stability. These two parts require serious independent research. Still, they fit into the context of this study's conclusions and suggestions, including its methodological chapter.

Under "intelligence" in C^4I, we mean, first, the EWS. Its influence in assessing the effectiveness of the command and control system as a whole is reflected in expectations of its reliability when making a timely report to the NCA of an enemy's nuclear missile attack underway. Without analyzing this problem in depth, let us note just one approach to this assessment.[226] In *A Model of the Effects of Warning on Stability*, Blair uses such a characteristic of EWS as Bayesian updating of attack model expectations, i.e. the probability of detection. After a statistical simulation of different scenarios, he arrives at a general conclusion regarding the complexity and ambivalence of EWS assessment:

> "The main implication that emerges from the Bayesian model is that conclusions drawn in a perfectly logical manner from incoming tactical information may be wrong even when the warning system performs to high standards. ... The result may be a positive control failure (due to insufficient confidence that an attack is under way) or a negative control failure (due to overconfidence)."[227]

An analysis of the EWS factor may be conducted to a considerable degree independently, without coordinating it with the assessment of other aspects of command and control systems mentioned. One way is to introduce, for the sake of simplicity, the probability of EWS working positively into the general assessment of C^3I (C^4I) as a value of 1.0. This corresponds better with the "pessimistic" approach of a potential attacker to planning the attack. But if we want to, and sufficiently trust EWS assessment, we can introduce the estimated probability of identifying the attack just as any other input parameter into the general connectivity graph. The method remains the same.

But even with such a logical assumption as the probability of EWS functioning being 1.0, and more than that, with the simultaneous assumption that the leadership would,

by all means, make a decision within the established time period, the problem in supporting the LOW posture does not get easier – the time allocated for all operational elements is too short. It seems that after all these arguments, the LOW posture should be cast off, especially if alternative LUA and DSS postures are able to provide reliable deterrence by themselves.

It is not, however, so simple. It is impossible to exclude the LOW posture physically. If all technical elements of the EWS remain in place (satellites, radars, computer centers, etc.), the possibility of reporting to the center also remains in place. To remove reporting altogether will be equal to depriving a human being of his eyes. If he gets hit, he will not even know who is hitting him. The goal of identifying the aggressor remains crucial.

The only solution for this situation is using the mentioned dual approach – that is, depending on which side is making a forecast. The potential victim will not conduct a "real" LOW due to the presence of reliable insurance (potential for LUA or DSS). But the potential aggressor will never believe it, because he knows that the opponent possesses an EWS. Quantitative assessment of the effectiveness of deterrence (in one specifically reviewed direction) will vary – the potential aggressor will make it higher and more redundant.

So, all the potential postures of nuclear weapons employment remain. A reasonably balanced way of spending is needed to provide for them.

Analyzing both LOW and LUA (DSS) postures on the basis of their stabilizing or destabilizing influence, we cannot help noting advantages and disadvantages in both of them. Some experts and officials prefer LOW because it realizes a much greater part of the nuclear potential, and therefore allows for certain reserves in the course of reductions in initial levels of strategic offensive forces. The supporters of this posture also add that there is no need to spend a lot of resources to increase the survivability of forces and command and control systems.

But significant expense in this case will be required to improve the warning systems. We saw that more than half of the former Soviet land-based EWS radars are located outside Russia. Some experts express general doubts about the possibility of creating a reliable EWS that can detect the beginning of an attack from all potential nuclear weapons locations.[228] Still, this is not the main disadvantage of the LOW posture. The main destabilizing factor in this posture is the necessity for the leadership to make a unique, highly-unusual decision to use nuclear weapons on the basis of data coming from technical sources and under the most severe time shortage – virtually a few minutes.

As for a LUA posture, the decision to conduct retaliation after establishing the fact of a specific attack is highly justified. Herein lies the permanently stabilizing effect of the LUA posture. The opponents of LUA argue, though, that another destabilizing element is present here: low retaliatory power or even its complete failure in case of the command and control system's decapitation. Accordingly, reliance on this posture may slow down the pace of reductions of strategic offensive forces.

It seems at first that each posture has both stabilizing and destabilizing elements, and the choice should be really made on the basis of cost – use whatever is cheaper. It is hard not to notice, though, that the disadvantages of the postures belong to different categories. If, using LUA, we can talk about a small scale of retaliation (for example, a certain number of warheads on targets), for LOW the exact magnitude of the strike is not that important (it is super redundant). The destabilizing moment here is a much more abstract one – it is the unpredictability of human reaction to a uniquely stressful situation. In the first case we may discuss the "real" meaning of some value (indicator of deterrence, stability, etc.); in the second case it is very hard to calculate. This leads to the conclusion that it is easier to "calculate" the LUA posture, quantitatively, than the LOW. This is important considering the goal: finding a reasonable minimum of strategic offensive forces.

If it is impossible to exclude one of the postures altogether, *how* to plan their use is a concrete and practical goal. We can find a clear, straightforward solution here: the main activity, planned for implementation in case of a crisis, should become retaliatory actions in the form of LUA or DSS. This should be the main intention written in the combat plans of the strategic forces' command posts. That, of course, requires a certain grouping of the nuclear triad to provide for effective deterrence within the framework of LUA (DSS).

Neither the United States nor Russia has yet made any official statements about general adherence to LUA (DSS). It looks like both nuclear superpowers continue to consider LOW their mainstay. This may certainly be explained by pessimistic estimations of the performance of their own nuclear forces and C^3 during retaliatory actions. This approach, however, dates back to the Cold War and is not relevant for the present day. As of today, negative control is obviously a priority, and the emphasis should be reversed. The proposed scheme, LUA-DSS (LOW), or launch only when a real attack (where the potential in principle for LOW is an additional deterrent) seems more logical at the time. Its guarantee against error is more reliable; at the same time, it preserves a sufficient level of deterrence.

It is necessary to remember that the process of developing and reorganizing the command and control systems takes many years and is characterized by considerable inertia. Thus, if decisions on prospective C^3I doctrine are not taken in the near future, it is possible for Russia to find itself, for technical reasons, a prisoner of a dated nuclear strategy in the years 2007-2008. Insufficient numbers of the components needed to provide for LUA (DSS) in command and control systems will continue to make an immediate reaction to EWS data the only useful concept, which will conflict with the changed character of nuclear forces on both sides.

The U.S. nuclear structure, with its main emphasis on the sea-based leg of the triad and special TACAMO-type and other command and control systems, corresponds to a certain degree with the LUA and DSS postures. But the high development of all American command and control elements, including EWS, guarantees reliable retalia-

tory actions under any posture, including LOW. It seems that as of today conditions in the United States are more favorable for official implementation of the conceptual plan, LUA-DSS (LOW). Effective civilian control over the Armed Forces and considerable spending for C³I have allowed a deeper understanding of the nature of the problem, and provide for flexible strategy in this area. This means that the U.S. nuclear forces and command and control have not only the ability to execute LOW, but also the ability to preserve a certain part of the nuclear potential after the enemy's attack, in order to analyze the situation and retaliate in a more purposeful manner. American experts see LUA, i.e., immediate retaliation after the reliable identification of the enemy's nuclear attack, as preferable, whereas DSS is perceived as a separate potential alternative.

Russia's command and control system was created with the main emphasis on LOW. No technical means were, in reality, created to implement LUA or DSS. At the present time, Russia is being strongly "pushed" toward the hypothetical situation of taking retaliatory actions in the course of an already carried out nuclear attack. This process is not a consciously established policy of the Moscow leadership but is developing almost automatically under the influence of the mentioned external factors: degradation of the land-based part of the Soviet EWS, a much more rigid time limit for decision-making than in the United States, and the necessity to obtain additional agreements from the Ukrainian, Kazakhstani and Belarusian governments, mentioned in Chapter 1. (Nobody has cancelled this agreement in the Commonwealth of Independent States; yet in the Norwegian missile episode, no one in Russia tried to coordinate his actions with the leaders of these independent states.) If, in the course of future reductions of strategic arsenals, SSBNs and mobile complexes became the basis of Russia's nuclear forces (by the general number of warheads), rushing into retaliation during the enemy's attack would make much less operational sense.

Subjectively, a part of the Russian military establishment is gradually being drawn to the LUA (LOW) scenario (i.e., there will be conditions for LUA but LOW could possibly be conducted), and away from LOW. Objective reality, though, makes the more challenging goal of providing for an effective DSS part of the agenda. The time, it seems, has arrived for Russia's leadership to adjust its strategic nuclear plans and pay more attention to the country's ability to function under the real conditions of a nuclear attack, not only at the moment of warning.

This forced transition to LUA and DSS raises the questions of how well, in reality, the Russian command and control system corresponds to the conditions of nuclear war, and what is the level of retaliation produced by this system. Two factors are of importance here: first, the presence of components that can provide, under unique conditions, the ability to issue an order to launch Russian missiles with a high level of probability; and second, the system's ability to deliver this order to the maximum number of missiles, which determines the power of the retaliatory strike (the number of launched warheads). If these questions are not resolved positively, the strategic situa-

tion may be assessed as unstable, including factors that would unavoidably lure Russia to use LOW.

Today's Russian command and control system already possesses some elements for functioning under conditions of nuclear war, such as the *Perimetr* subsystem. These elements, containing components of increased survivability, reach out, so to speak, to the silo-based and mobile missiles, but they are not meant for transmitting orders to submarines. One can state with high confidence that until deep reductions of SRF are implemented, the expected level of Russian retaliation will continue to be sufficient to provide a reliable deterrent. Still, in the nearest future, the problem of command and control for submarines must be resolved, and performance within the framework of LUA and DSS should be provided for in a more reliable way. The only alternative is a cardinal change to the minimal required level of retaliation that would serve as a sufficient deterrent.

The general principles of employment of strategic forces are discussed in a fundamental study by a group of Russian scholars, edited by Pavel Podvig. While the information in the book is valuable, and its publication in Russia is significant by itself, some comments regarding the concepts of SNF employment are called for.[229]

The authors of the study say that "launch on warning ... may appear to be a justified strategy under certain conditions." This phrase may be understood literally by some not-very-well informed readers. Unfortunately, the subsequent explanations fail to demonstrate that this option is absolutely inadmissible.

One cannot completely agree with the statement that "... in case of launch-under-attack, unlike in case of launch-on-warning, the decision to use nuclear forces would be based on the real fact of the beginning of a nuclear attack, recorded by the warning system ..."[230] As we have noted earlier, information obtained by the EWS should never be enough to immediately trigger a massive retaliatory nuclear strike. It is another matter that the possibility, in principle, of such an uncontrolled, random reaction of the opposite side has to be taken into consideration by a potential aggressor, thus strengthening deterrence.

Finally, under the LOW posture the NCA have "no more than eight to 10 minutes," as maintained by the authors of the study cited above, but only two to three minutes. This opinion is shared by the absolute majority of Russian and non-Russian experts.

Despite some inaccuracies noted above, the ideas regarding the principles of employment of SNF, found in the study edited by Podvig, are interesting.

The question of a retaliation threshold or, as it is sometimes called, the level of unacceptable damage, is as old as it is complicated. All the criticism of LUA and DSS has always been, and still is, based on the idea of allegedly "low" level and probability of retaliation. In order to justify LUA and DSS, and thus significantly increase strategic stability, the military mentality on both sides of the Atlantic should undergo considerable changes. For ordinary people, an unacceptable damage level is not hundreds or dozens of nuclear explosions, but probably even a single digit number of these – all the

more so since the targets that will be struck are not known in advance (everyone is a hostage).

With the planned arms reductions, we are very far from such low numbers for hypothetical retaliation. At least, it is clear so far that according to calculations a retaliatory strike would involve these same hundreds of warheads. It is evident that the key to the problem of nuclear disarmament is in coordinating a gradual reduction in the level of "acceptable" nuclear retaliation for each side.

A practical step toward solving this problem of nuclear employment postures would be for Russia to recognize LUA and DSS, not LOW, as its mainstay postures, and official confirmation that Russia does have certain reserve systems for command and control under conditions of nuclear war. It would serve a good purpose to make this announcement publicly but without stating the specific numbers and locations of the mentioned components. Even a demonstration of some parts of these components would be possible (just as it is done now for many types of missiles).

At the same time, it would be desirable for the United States to also confirm its reliance on LUA and DSS, and exclude from its combat plans an immediate nuclear reaction to EWS information. Some American experts already see such a transition as a positive step: "Most important, the threat of a surprise nuclear attack, which was the touchstone of traditional arms control theory, can no longer be considered even a viable planning scenario."[231]

As of now, Russia possesses certain technical capabilities for modernizing its C^3I system in a direction well designed to fit the context of nuclear disarmament. Based on this conceptual foundation, those scenarios reviewed above, for detargeting as well as undocking warheads from missiles, will seem much more logical and purposeful, since the unavoidable reduction in readiness will be balanced by a guaranteed capability to operate in extraordinary circumstances. From a national security standpoint, such measures as a ban on removal of Russian rail-based ICBMs from their garrisons, bombers' watch without nuclear weapons, reduction in OPTEMPO of SSBNs by increasing the time spent in port, or watch of air-based command and control posts spent on the ground will look much more justified. It is possible that a mutual official transition to the LUA-DSS (LOW) posture would allow for more rapid methods of nuclear disarmament without the considerable expense of proportionate decommissioning of delivery vehicles.

Blair suggests that strategic stability can be strengthened only (or mostly) by reducing the combat readiness of nuclear forces within the framework of zero alert. He is quite skeptical regarding measures to strengthen the system of command and control because they serve, in the final analysis, the goals of strengthening not safety, but deterrence:

> "But in the final analysis all the command and control arrangements discussed here sustain alert practices and emergency launch procedures whose main purpose is to service deterrence, not safety ... The operational posture would have to eliminate its dependence on strategic and tactical warning, and launch under attack ... Strategic

forces would be taken off alert and the hair trigger removed from the nuclear command system."[232]

One cannot fully agree with this approach. What if, even after mutual deep reductions of readiness, there is a return to confrontation? Reliable positive control also strengthens safety. The heart of the matter is whether the measures of positive control introduce additional instability or not. If a measure of positive control is satisfactory from the point of view of negative control, then it should be viewed as a good one, and utilized. For example, the *Perimetr* system's existence does not damage the effectiveness of negative control, but definitely strengthens strategic stability. Therefore, transition from a "hair trigger" posture to the more rational LUA or DSS postures is sufficiently realistic. (Of course, if one views the idea of nuclear deterrence itself as rational.)

However, taking into account the fact that one cannot do without concepts of nuclear employment in general, Blair views as acceptable in principle the posture of "delayed retaliation" or the so-called end-state stability:

"End-state stability has one basic component. Having reached a state of maximum combat readiness, the command systems should be able to support a strategy of delayed retaliation. This means that the established wartime mission of the nuclear forces could be accomplished without resort to launch on warning or launch under attack ... The U.S. strategic nuclear forces have never been able to meet this requirement."[233]

The suggested official reorientation of nuclear weapon use postures is most certainly impossible without a preliminary mutual agreement between the parties on preservation of national security at the expense of reliable (unfortunately, for now) mutual deterrence. So far, no steps have been made in the direction of such an agreement. At the same time, it is quite probable that as soon as Russian and U.S. experts begin their calculations together in a cooperative spirit, the possibility of relying on LUA (DSS) could arise. After that, we could try to predict the future by coordinating a balanced level of deterrence with implementation of new deep reductions.

As becomes clear from this section, detargeting, reducing combat readiness of nuclear forces and employment postures are tightly linked in one knot through command and control systems. For example, detargeting, with the resulting reduction in readiness, is directly related to the question of postures. Or, LOW demands a high level of readiness to achieve fast reaction, while to support LUA (DSS) another aspect of readiness, survivability, is emphasized, etc. Any strong trend toward one of the postures will be negatively reflected by other requirements.

There is no sense in arguing against mutual reduction of combat readiness for nuclear forces (as is being partially done now) and their command and control systems. Blair,

one of the most active supporters of this approach, notes that introduction of the zero alert regime for nuclear forces may have a beneficial influence on the problems of C^3: "One of the important features of zero alert is of course that it reduces, in the first instance, the chances and consequences of Russia's losing control over its nuclear weapons. Zero alert serves as a buffer against contingencies that pose far greater danger when nuclear forces are kept on launch-ready alert."[234]

Under zero alert, C^3 systems themselves should be organized to exclude an uncontrollable diffusion of command and control during crisis periods, and to make the transition to higher levels of readiness a real prerogative of national leadership: "This strengthens top-level control over the process and inhibits spontaneous escalation."[235]

Blair, when discussing close correlations between various aspects of nuclear weapons control, notes the necessity to think through carefully how to avoid creating any dangerous superiority for one side in case when high degrees of nuclear forces readiness must urgently be restored:

> "Any zero-alert procedure must pass a test of peacetime and crisis stability. The first par of the test is simple: does the plan remove the ability of potential adversaries to mount a decisive sudden attack in peacetime? The second par is more complex. The postures must provide for transitional stability during the regeneration of nuclear forces in an emergency and ensure that the process bringing forces to peak readiness culminates in a stable balance between them."[236]

Evidently, it is not the easiest task. Blair even believes that in the process of regeneration of higher readiness the sides must not race against each other, but, on the contrary, help each other if necessary: "But the regeneration of strategic capability could well be an inappropriate response. If Russian nuclear control convulses under internal pressures, the Western response should, at least initially, be to provide reassurance and even assistance, even though the situation might increase the nuclear threat to the West."[237]

It is a good proposal, but one would like to have something else in reserve. One tool for providing strategic stability under continuous fluctuations in forces' readiness would be the prognosis of results of military contingencies, in various regeneration scenarios for strategic forces. For example: will I have an advantage if I get ahead of the enemy in regenerating nuclear forces, or not?

To paraphrase, under this type of zero alert (that is with additional insurance), the sides could have reliable negative control in reality and no less reliable positive control on paper (in a model jointly developed by both sides). This posture option seems much more preferable than the one we have today.

5.4 Predelegation

The possibility that authority for using nuclear weapons can be delegated under

certain circumstances from a political leader to lower levels in the command hierarchy is an important problem for any C^3 system. This can be seen most clearly by the unity of opposites in the "negative control – positive control" bipolar system: With total centralization, the level of negative control is the highest ("super PAL" according to Sagan),[238] but the danger of the system's decapitation is great. And at the opposite end, the lower the delegation of authority can go down a command and control system, the higher the system's survivability, i.e. positive control; but accordingly, protection from unauthorized actions is lower.

American experts and officials pay considerable attention to finding solutions for this problem. Feaver discusses this question in great detail.[239] He reviews two methods of delegating authority down the chain: devolution of command – delegating command and control; and predelegation of authority – delegating authority in advance. In both cases, according to this author, command and control is transferred from civilians to the military.

In principle, delegation of command and control is perceived as a legal, widely used practice. The president, as commander in chief, has the right to delegate his functions to his subordinates. Devolution of command also includes those cases when, if the higher commander is incapacitated, the lower level of command accepts his responsibilities.

In the United States, the devolution of command is under constant careful civilian control. In peacetime, the secretary of defense is only the sixth in the constitutional chain of command for the president's successors. But during crisis periods, there is a strong motivation to "sneak around" the constitutional chain and devolve command to the Joint Chiefs of Staff and strategic commanders in chief, who, according to Feaver, have much more competence in questions of nuclear conflict than the secretary of the interior.

Nevertheless, the dubious legality of such plans is noted. The author cites a number of historical examples when parts of the presidential command functions were, without public knowledge, devolved to commanders of strategic forces, and lower level commanders were ready to use nuclear weapons at their discretion "under certain circumstances."[240] The author is hopeful that today the U.S. government does not have such plans because they are both unconstitutional, politically undesirable and could possibly begin a slide into nuclear war:

> "The decision to use nuclear weapons, and by extension the determination of the circumstances under which nuclear weapons will be used, is considered to be quintessentially political in form and substance. In a democracy, the military simply do not have the right to make such a decision, regardless of whether those who do have the right decide to cede it to the military."[241]

The exclusive prerogative of the national leadership to authorize the use of nuclear

weapons is seen as a supplemental measure to increase civilian control over nuclear weapons. In this case, predelegation – prior delegation of nuclear release authority to military commanders – is permitted. The author feels that this constitutional right of the president is strategically justified and increases deterrence. Opinions of the military on this issue are cited: "In light of this vulnerability of portions of the strategic arsenals, Gen. Nathan Twining, former chairman of the JCS, defended predelegation as 'the only solution to military fire control'."[242]

At the same time, Feaver addresses the dark side of this function. He notes, with good reason, that implementing predelegation introduces great "automatism" into the subsequent actions of lower command levels. Quoting Paul Bracken, he expresses his concerns that the delegation of nuclear responsibilities may occur at such a moment in the crisis when the political leadership is ready to compromise. And at this moment, the military, making its decision on the basis of an unfavorable military situation, may use predelegated nuclear release authority to avoid the damage that politicians may find acceptable.[243] In this regard, he reminds us that World War I began because the civilian leadership of opposing countries lost control over the situation.

Another potential danger is the fact that, after certain levels of the military command receive authorization codes, it would be practically impossible to distinguish between "legitimate," i.e. authorized by national leadership, and "illegitimate" launch orders.

Reversing the codes back to the leadership level in case of peaceful resolution of a crisis will also be extremely difficult, including purely technical difficulties. It is necessary to exclude even the slightest possibility of compromising these codes and any opportunity for their unauthorized use in the future. This is probably solvable only through a total replacement of the old codes with new ones, which brings certain organizational difficulties.

Feaver also notes that since predelegation plans (if they even exist) are known only to a very narrow circle of high officials, the level of the command and control chain at which a legitimate order could be distinguishable from an unauthorized one would remain very high. (One can assume that the author probably means the level of commanders in chief, where there are many various sources of sufficiently reliable information.) He mentions widely spread public speculation about this delicate subject, namely the U.S. government's reluctance to describe the "space of predelegation" more or less specifically.

It is thought in the United States that the first most significant step toward delegating nuclear authority to the commanders in chief was made by President Dwight Eisenhower. This decision was maintained by his successors. Feaver cites another American expert:

> "Daniel Ellsberg asserted that Presidents Eisenhower, Kennedy, and Johnson predelegated authority to six or seven three and four star generals, that is, the unified and specified commanders. Ellsberg's claim appears to be supported by a un-

> classified memo written by McGeorge Bundy for President Kennedy in which he warned about policies that enabled a senior military commandeer to use nuclear weapons in the absence of a presidential order."[244]

Blair says, "In pursuing a rapid reaction posture, the United States delegated nuclear launch authority to military commanders during the entire Cold War era."[245]

The majority of experts believe that the situation has not changed since, even though there is no official confirmation of this policy: "Predelegation, while conceptually straightforward, would actually be extremely difficult to operationalize. It raises profound questions about how far down the chain of command the authority should be delegated, how wide discretion should be granted, and how authority would revert to the civilian leadership. ..."[246]

As mentioned, the range of delegation and the very existence of such plans is kept secret. Sagan comments on the same subject: "The precise details of how successive presidents have chosen to balance those competing requirements is among the government's most highly classified secrets. ..."[247]

First, it is understandable, since we are talking about the prediction of negative control effectiveness. Let us, however, note that the level of delegating may be changed at any time depending on necessity, even though in only one direction: down. And second, the possibility to delegate nuclear authority may make one hopeful that the survivability of command and control will increase dramatically in the crucial moment of any crisis, which in turn increases the deterrence factor. It serves no purpose and is totally senseless to conceal this. In this vein, Sagan continues: "It would be wildly imprudent for Soviet leaders to assume, however, that destroying Washington in an initial nuclear attack would ensure that retaliation would be eliminated. (It would be equally impudent for U.S. leaders to assume that destroying Moscow in a 'decapitating' attack would eliminate the risk of retaliation.)"[248]

It seems that – as with many other aspects of such a strange subject as nuclear deterrence, one that is unusual for standard assessments – a lot here is based on lack of certainty.

It is extremely important that the possibility of delegating nuclear authority from the top political leadership to the military command at any level, all the way down to the execution level, cannot be totally excluded by any organizational or technical measures, even if everybody wants to execute this. From the point of view of negative control this situation is very bad. But this is a real fact which cannot be ignored, and should be considered not only in the qualitative but also in its quantitative aspect, whenever possible.

It is not very hard to take into account the potential of predelegation in quantitative estimates of deterrence. Predelegation simply changes the connectivity graph considered in Chapter 3. If under a rigidly centralized command and control system we are dealing with a "pyramid," predelegation "breaks" it. Let us assume that the potential

aggressor, when evaluating the risks of a nuclear attack against the United States, should consider as a fact the launching potential of commanders in chief as well as that of all SSBNs. His strike would be planned with these considerations in mind. With a more cautious "pessimistic" prognosis, he should count on the worst-case scenario for himself – that this potential would be delegated all the way down to LCCs at the last moment. Thus, the plan of the attack has to be changed again, etc.

Some optimal level of delegation, which does not undermine negative control too much and preserves the reliability of a launch order reaching the missiles sufficient for deterrence, probably exists. For peacetime and crisis conditions, this level should certainly vary. Should this level be proved scientifically, it could be officially published. All the more so since, as we have noted before, the "rational" opponent should base his estimates on the much more radical predelegation scenario for the opposing side – that is, the worst possible scenario for himself. What we have in this case is a well-known situation from game theory with two sides differently evaluating the same prognosis.

At this point it would make sense to look at some American experts' evaluations of nuclear delegation in Russia (Soviet Union).

It was emphasized in preceding chapters that Russian C^3 is mostly viewed as being very centralized. Since we cannot completely rule out delegation as a hypothetical option, we reach the same conclusion that we were able to reach regarding the U.S. C^3: there is no guarantee for a potential attacker that the opposing side will not carry out such a predelegation at some point. We do not mean here specific intent of the attacked side (Russia, in this case); the important part is that the potential aggressor has to think that way.

There are no technical problems with predelegation in the Russian C^3 system. All it takes is transmitting the authorizing codes (encryptions) in the usual way, with the addresses of corresponding levels in the command and control system. The problems, just like in the U.S. C^3 system, are rooted in the opposite requirements of negative and positive controls.

The dilemma of predelegation is most complicated when it comes to command and control of TNW. By the end of 1990s, the United States had several hundred tactical nuclear weapons (TNW) in Europe (B-61 gravity bombs), and about 1,000 TNW in the United States, including 350 nuclear-armed submarine-launched cruise missiles. By the same time, Russia had an arsenal of TNW in the range of 3,000 to 4,000: nuclear gravity bombs, nuclear artillery shells, warheads of anti-aircraft missiles and missiles of different types. All TNW owned by both countries are kept during peacetime in special storage facilities, but during a threat period they are supposed to be deployed with appropriate military units in theaters of military action. Each TNW has a blocking device against accidental use or unauthorized actions, and it can be used in combat only after an appropriate sanction from above, with appropriate codes permitting their employment. I will not attempt to evaluate the reliability of such a safety system, although one may raise certain questions regarding the difficulty of guarding and servicing TNW at the bases of conventional

forces. I would like to consider here only the operational aspect of the TNW problem.

The character of combat employment of TNW is substantially different from the concepts of SNF employment, discussed in sufficient detail in this book. The main principle of SNF employment is rigid centralization of command and control, and simultaneous release of the launch sanction to all involved SNF components, based on the sanction by the nation's chief executive. The operational requirements for TNW would make such an approach senseless. Indeed, a commander in the field would find out faster and better how and when to use TNW; he is more aware of the situation than his superiors, and is vastly better aware of it than the NCA. Naturally, the situation would differ in various theater parts of military action, both in time and in space. The NCA would find it extremely difficult, perhaps even impossible, to determine the thin line between the two extremes: Avoid TNW use and risk a decisive defeat in a conventional war, or, while still capable of conducting conventional warfare, hurry to order the use of weapons of last resort, and thus cause an adequate response with inevitable escalation of nuclear conflict up to the global level. Obviously, it would be sheer madness to give field commanders, in a situation far from clear, the authority to use TNW according to their judgment.

One may say, of course, that NCA would have a similar problem deciding when to use, if forced by circumstances, SNF, and that in principle it is possible to release a sanction to all combined arms formations for employment of TNW. This, of course, will no longer be a selective use of the more effective weapon at one sector of a theater in order to achieve a tactical goal, but in fact employment of TNW in a strategic operation by SNF. Thus, it would be simply an addition of a series of less powerful nuclear explosions to the already ruinous planetary nuclear catastrophe, since it is impossible to imagine a war employing only TNW. Does one really need such a second helping?

Today, it is often said that Russia needs to preserve its TNW in order to balance the large advantages of its neighbors (NATO, China, etc.) in conventional forces. This makes sense only as an addition to Russia's SNF. If we view this issue only through the prism of the C^3 factor (leaving all other strategic aspects aside), we must conclude that TNW, in Russia as well as all other nations, should better be eliminated both because it is difficult to provide for their negative control when in storage and in the field, and because its operational command and control are not flexible enough.

The situation with SNF is different. Working on improving their predelegation system, the Russian military and research and development specialists chose a method different from the Americans. Its main idea was to keep the highest possible degree of centralization, while at the same time providing for maximum survivability of the commanding organ that has the authority and technical potential for launching the missiles. This idea was implemented in *Perimetr*, described in Chapter 4.

Blair paid a lot of attention to analyzing the role and place of this system in nuclear deterrence. He briefly describes its idea and its operational significance.[249] In general, he assesses the system positively, indicating that it allows for realization of the

leadership's right to err:

> "From the standpoint of safety it would be more prudent for the Russians to withhold a launch decision, activate the Dead Hand in response to tactical warning, and predicate a final launch order on evidence of nuclear explosions ... In sum, launch under attack using the Dead Hand permits an initial mistake (false alarm or misinterpretation of warning sensor data) to be corrected by the absence of nuclear explosions."[250]

It would be useful to mention here the two articles published in *The New York Times*. In October 1993, Blair described briefly and, as a whole, correctly, the *Perimetr* system. Yet, he expressed his concern that the system increases the risk for unauthorized use of nuclear weapons especially during crisis periods.[251] By the time his article was published, the existence of the system in Russia and various evaluations of its significance had been already mentioned in American writings.[252] To prevent erroneous speculation on this subject, I responded to Blair in *The New York Times* on Feb. 1, 1994.[253] The idea of my commentary on Blair's article was that *Perimetr* not only does not weaken negative control, but, on the contrary, is built to improve its reliability during very acute moments of crisis and therefore it plays an exclusively stabilizing role.

Having this system at their disposal, Moscow's political and military leaders now have more freedom not to rush into action upon receiving signals of an attack from the EWS. As was shown in Chapter 4, they may, at this critical moment of uncertainty, delegate the launching function to special highly survivable nodes of the command and control system without sacrificing the reliability of direct measures to protect against unauthorized actions. In reality, negative control is strengthened because this type of "insurance" relieves authorized officials from the difficult dilemma of making a choice in a stressed, changing and totally unique situation.

In one of his later works, Blair essentially recognized the rationality of the idea at the core of *Perimetr*: "The rationale for this Dead Hand system is evident."[254]

After coming to this conclusion, Blair attempts to analyze some operational aspects of the system's employment, relying here on information received from four knowledgeable, high-ranking Russian experts from the Main Operational Directorate of the General Staff and industrial ministries.[255] All four confirmed the existence of the system. Two of them stated that it provides two technically-possible scenarios of operation when on duty: the first is to include sensor information registering occurrence of nuclear detonations into *Perimetr*'s main algorithm; the second bypasses the sensors, relying simply on transmitting, at the necessary moment, authorization codes from Central Command Posts to the system's command missiles. Two other experts denied that the sensor scenario is operated while on duty, though they confirmed that the system possesses this capability. They mentioned Marshal Sergei Akhromeev, the former chief of the General Staff, who allegedly rejected operational use of sensors for safety considerations.

In any case, the *Perimetr* does exist and possesses the technical capabilities described above. It is not necessary to know the precise variant of its operation that is used when the system is on duty, all the more so since it can always be changed according to circumstances. Even switching the system off, taking it off duty, does not change anything. Its existence will force any potential aggressor to evaluate Russian C^3 in a different way under the difficult conditions of a hypothetical nuclear conflict.

Indeed, when the *Perimetr* system is taken into consideration, the connectivity graph in the simulating model becomes very different. Without it, all orders arrive at the ICBMs' launchers only through the command posts of the missile regiments (UKP), but when *Perimetr* is operating, the orders, as already emphasized, arrive directly from command missiles, bypassing all intermediate levels of the command and control system. In other words, alternative ways make total suppression of the connectivity graph much harder. If we remember that the command missiles are launched from dispersed groups of highly survivable launchers, the degree to which the reliability of Russia's command and control system is strengthened becomes evident.

Besides *Perimetr*, there are other possibilities to delegate nuclear release authority down the system at a critical moment in order to expand the connectivity graph to its maximum. These do not characterize only Russian command and control. The C^3 systems of all nuclear states have such capabilities and they cannot be eliminated. For example, it is impossible to exclude a situation in which, at the most difficult moment of combat actions, the commander of a missile unit already possessing nuclear authority delegated from above would decide to delegate them to the very bottom level – that is, down to the launchers themselves – for the sake of "greater reliability." In truth, this example belongs rather to the area of devolution of command and control at the lower level than to the area of delegation, but, for simplicity, we are going to treat it as an example for predelegation.

In the Soviet Union, this concept was implemented through "autonomous launches." These were constantly practiced during military exercises. At a certain moment in combat actions with conventional weapons, or during the threat period, the commander of a division of silo-based ICBMs sent to each launcher without a crew (a so-called *otdel'nyy start* – separate launch) a specially trained unit headed by an officer (*raschet avtonomnogo puska* – autonomous launch crew). This unit was stationed at an underground bunker that had been prepared in advance in the vicinity of the launcher. The unit did not deliver any codes, in order to avoid reducing the reliability of negative control. The unit did, however, have with it an ultra-short wave radio transmitter-receiver, keys and passwords to enter the silo, and a special miniature device for launching the missile (PAP – *pul't avtonomnogo puska*). When the higher command sent down an appropriate order, this unit would receive the launching code on the radio (that same code that in ordinary circumstances should have been transmitted via an underground cable from the regiment's command post). This code could have been transmitted to them from any of the surviving command posts of the division, including the

regimental level, or even from an airborne command post of the missile army, if the latter found itself in the area of the division and at a distance allowing permanent communication on the ultra-short wave radio.

I had the opportunity to observe training for this scenario several times during exercises. The unit arrived in the vicinity of the launcher in two cars, and consisted of three to four people. After receiving – by radio – the authorization code (with simulated "jamming" by the enemy), the unit entered the silo, introduced the code into the special miniature device and transmitted the launching order to the missile. Then the unit left the silo rapidly, and drove away to a safe distance as soon as possible. It took several dozens of seconds from transmitting the order to the missile until it would leave the silo. Once, one car broke down and the whole unit left the launching area in the second car. According to the conditions of the exercises, the autonomous launch crew had to have two cars. Other necessary safety measures were also used.

In difficult conditions of combat situations, these and other methods of delegation improve the effectiveness of retaliatory actions. Thus, a command and control system "milks" the highest number of surviving missiles in each area of deployment, including them in the general balance of retaliation. Judging by the description above, negative control does not suffer dramatically. At least it does not decrease any more than is necessary in combat actions, when positive control acquires the most importance.

To conclude this section, let us note again the need to separate two questions. First, the ability of the potential victim to use all forces and means it possesses, an ability that the potential aggressor cannot help considering when analyzing its plans. Assessments of levels of mutual deterrence should be done from this point of view. And, second, practical implementation of the delegation potential. It is evident that the latter can be viewed only in the context of the realities of a nuclear crisis itself. The most important part of the second issue is assessment of delegation potential with emphasis on maintaining reliable negative control in peacetime.

5.5 Uncertainty: Deterrence or Provocation?

The previous sections demonstrated how closely knit the various aspects of nuclear command and control are. This is characteristic of C^3 problems and makes analysis quite difficult. This difficulty is also increased by the lack of any clear answers to most questions at the present time. What we are dealing with is, in fact, uncertainty. We can name a whole series of such questions:

- How do we establish and implement the "golden mean" between requirements of positive and negative control – that is, overcome the "usability paradox"?[256]
- How much survivability should C^3 have in order to overcome any dangerous illusion of its weakness? And, in this regard, should we be thinking about various "justifying" conditions for the employment of nuclear weapons in a first strike?
- Is the goal of mutual detargeting realistic from the standpoint of mutually effec-

tive verification, or is it purely a political bluff? And what would be the "acceptable" ethics of targeting? That is, what should be established as targets for a retaliatory strike: the attacker's empty missile silos or something else? How does it fit into the concept of deterrence?

- Can we rely on information from the EWS about a missile attack in progress so much that we retaliate with an immediate nuclear strike (choice of postures)?
- How much could the readiness of nuclear forces and their command and control systems be reduced without permanent damage to national security, and what guarantees are possible here?
- How do we conduct quantitative analyses of the contribution of C^3 to the balance of deterrence and strategic stability, considering the prospects of deeper reductions in strategic offensive forces and the desire to minimize expenses for nuclear forces in general? Does a consistent theory of the part and place of C^3 in all these matters exist?
- Are openness and international cooperation between C^3 experts in this area useful?

We could continue this series of questions, most of which do not have any convincing answers so far. This work also does not give answers, but it attempts to attract attention to the necessity of starting a serious study by Russian and U.S. experts, and finding solutions to these problems.

Lack of certainty in nuclear command and control issues has always been damaging for strategic stability. During the Cold War, uncertainties justified new spirals in the arms race and increased international tensions. At the present time, it is a hindrance to reduction of nuclear arsenals, and prevents a decisive transition to mutual deep reduction in readiness for the remaining nuclear forces. Due to the lack of certainty in command and control issues, both sides continue to cling to the outdated posture of LOW, and at the same time admit that this is not the best choice at all.

Unfortunately, these are not all the disadvantages of uncertainty. Lack of certainty in C^3 and related doctrines of nuclear weapons use results in certain over-insurance on both sides and reconsideration of arms control agreements achieved earlier. The actions of both the U.S. and Russian political leadership are not always in harmony with the goals of disarmament and global stability, thereby provoking criticism from the experts and the public. Blair's report, *The Effects of U.S. Policy on Russian Nuclear Control,*[257] is a typical reaction of C^3 experts to current political activity in both countries.

Blair's general conclusion is that the U.S. policy toward Russia was wrong, forcing the latter to take responsive measures that made the situation worse in general, and regarding reliability of negative control in particular: "Although U.S. security depends on ironclad Russian control over nuclear weapons and materials, our security policy toward Russia does not promote the strengthening of that control. In fact virtually all facets of our policy, except for the Nunn-Lugar program, work against it."[258]

Blair notes that the Russian C^3 system is going through hard times even without the

influence of any external factors. The fall of the Soviet Union and economic instability in Russia, reduced cohesion of the Russian military and politicians at the top levels of C^3, as well as some other factors, have caused serious problems for both positive and negative control. He states that Russia continues to adhere to the posture of LOW and that "... risk of a breakdown of control has been steadily rising in several dimensions."

According to Blair, however, this situation is made worse by such current U.S. policies as:

- maintaining the same level of high combat readiness for nuclear forces which, according to experts, will provide serious superiority over Russian nuclear forces in case of a nuclear conflict;
- continuing reliance on the unnecessary long-term concept of nuclear hedging;
- persistently pushing for the expansion of potential missile defense for North America, and in the possible theaters of military operations;
- encouraging NATO's expansion eastward;
- taking a rigid position at the START negotiations;
- continuing activities in such areas as preparation for strategic anti-submarine warfare.

Naturally, says Blair, such and similar actions by the United States result in corresponding measures by Russia. In particular, he noted the increase in number of SNF exercises, including deployment of mobile ICBMs into the field, SLBM launches, and training elements of the nuclear forces under LOW conditions. These actions increase the danger of a breakdown in negative control. He also notes that Moscow is afraid that, under the cover of the BMD program, the United States will create a shield which will bring down to zero the effectiveness of Russian retaliatory strikes. In his opinion, it can even bring back the concept of a pre-emptive nuclear strike. As for the START negotiations, by forcing Russia to switch to mobile components of nuclear forces, the United States made the situation worse regarding protection from unauthorized actions, which is less reliable for Russian Topol (SS-25) and SSBNs than for silo-based ICBMs. NATO's expansion eastward can stimulate an increase in Russia's TNW, where the issues of negative control are even more challenging.

In the conclusion of his report, the American expert stressed the same idea that is central to the previous chapters of this book – the necessity of developing a more clear and definitive theoretical basis for the problems of nuclear weapons:

> "The various policies, operational practices, and real or imagined threats discussed above may seem academic in this post-Cold War era. They do seem to embody the tired old concepts of a previous era in US - Russian relations. The sort of calculations presented above seem rarefied indeed. But the fact remains that neither government has replaced the classical formulation of security based on strategic balance and de-

terrence, and therefore these principles continue to dominate the logic of nuclear planning, the operational postures, and all the other issues under discussion."[259]

Today, one may say that the American expert was right, at least regarding the Russian reaction to the actions by the United States. Of course, much has changed in U.S.-Russian relations since then, and the leaders of the two nations strive to avoid aggravations in relations. But the analysis cited above will continue to be useful: politicians must avoid actions that could make nuclear powers take dangerous countermeasures, some of which may be inadequate.

Continuing lack of certainty about many aspects of nuclear command and control and the shortsighted policy of the United States toward Russia discussed above create an atmosphere which allows certain circles in Moscow to talk, like they have for several years, about the possibility of Russia using nuclear weapons first, and, much worse, are trying to justify the necessary conditions for this.

In this regard, we can refer to an article by Maj. Gen. Vitaly Ryaboshapko in *Military Thought,* tellingly called "Conditions for a Transition to Potential Use of Nuclear Weapons."[260] The author, now retired from active duty, was an expert in the maintenance of strategic offensive systems in the SRF and, in the years just before his retirement, worked for the Center of Operational and Strategic Research of the General Staff. I worked side by side with him for a long time, and must say that he had always been very far from underestimating the consequences of nuclear war, and had been highly critical of the "hawks." Nevertheless, in the cited article he talks straightforwardly about the need for Russia to establish conditions under which it would be the first to use nuclear weapons as a response to an external threat to its national security.

There is no need to repeat here the contents of his article. It is clear that such conditions, developed unilaterally (not just by Russia, but by any nuclear state), would not have any international legal power, but the consequences of their application would still be catastrophic for the whole planet. Such conditions will probably never be formulated in Russia. But the very fact of the article's appearance in an official military publication demonstrates that some in Russia are looking for a potential way out of the situation, which is already complicated today and can become dangerous in the near future. The "way out" suggested in the article is, of course, unacceptable; they have to look for another one. The latter can be found only through friendly cooperation between the United States, Russia and other nuclear states, including a broad range of official and independent experts in the area of nuclear weapons and their command and control. An assessment of "justified" conditions for first use of nuclear weapons can be only performed multilaterally. Of course, it is necessary to look for a way out of this dead end, and the Russian expert is right in this regard. This way out, however, should be sought together by the nations concerned.

Some American sources cite differences of opinion or even conflicts between the military and civilians over the positive-negative control dilemma:

> "There are inherent trade-offs between positive and negative control, between ensuring that weapons will always work when one wants them to, and will never work when one does not ... The general trade-off is simply stated: the greater the assurance of 'always,' the lesser the assurance of 'never,' and vice-versa. The proper balance between the two is a subject of dispute between civilians and the military."[261]

I would like, however, to elaborate on this formula. Not very long ago, some people may have sincerely believed nuclear war and victory were possible. Now the situation is different. The majority in the militaries, including the heads of the SNF of Russia, the United States and other nuclear states, are not planning to really use these horrible weapons. Even if they continue parting the line of duty to improve positive control, it only means that they have to promote the policy of preserving mutual deterrence conducted by their civilian leadership.

The militaries are also involved in negative control of nuclear weapons, in all institutional and technical measures of protecting them against accidents and sabotage. They are much more involved in these aspects than the politicians. At the present time, the militaries face additional work in this area: implementing the agreements on strategic offensive forces reduction. Experience shows that these activities now take up no less time in the schedule of strategic commanders, their staff, command posts and services than their traditional military activity.

If cooperative research in C^3I (C^41, C^5I, etc.) issues and their contribution to strategic stability finally begins among nuclear states, the military experts will again play a considerable role. Therefore, the military and civilians should not oppose each other. After all, it was a civilian who issued the order to bomb Hiroshima and Nagasaki. And should nuclear weapons some day disappear from the face of the Earth, the military will experience as much relief as civilians.

Uncertainty in the area of nuclear command and control has a twofold role: it both deters and provokes. The deterrents are the unknown results, fear of the worst. The provocation is the secret hope for a "Maybe!" The latter seems less dangerous when nuclear potentials are huge and, as such, make people reluctant to experiment. But the deeper the reduction of strategic offensive forces, the more this provoking aspect of uncertainty will come to the forefront. If the sides seriously intend to move further toward nuclear disarmament, they should inevitably arrive at certain agreements and mutual assessments in that area of C^3I.

Sharp debates among experts and political struggle at the highest level – both inside the United States and Russia as well as between the two – accompanied the work on NMD in the United States and the American decision to withdraw from the 1972 Anti-Ballistic Missile Treaty (ABM). Until it became clear that the United States would withdraw from the treaty, Russia was adamantly against any concessions, fearing that NMD would eliminate Russia's retaliatory potential, especially when deep cuts of its

nuclear arsenal occur either as a result of arms control agreements or spontaneously. The former SRF commander in chief, Yakovlev, said:

> "All the talk about 'modification' of the ABM Treaty is misleading. The deployment of anti-ballistic missiles constitutes denial of the treaty's essence, since it will allow protecting 70 percent of the U.S. territory. And we have no guarantees that the next step will not be five or six more similar deployments, since increasing the number of interceptors becomes a purely technical matter once the information system is created. This will completely ruin the existing U.S.-Russian nuclear balance: the force co-relationship, when NMD is taken into account, will become 10-to-1 or even 15-to-1 in favor of the United States, depending on the configuration of the NMD."[262]

Yakovlev is absolutely right in saying that increasing the numbers of interceptors will be a purely technical matter. And the principle, laid in the foundation of the ABM Treaty, is also correct: Mutual deterrence due to inability to escape retaliation. However, I believe that this fundamental principle will work as well under conditions of *any* BMD system. The crux of the matter is our assessment of BMD effectiveness.

Indeed, if we select, out of thousands of modeling simulations of retaliation, the most characteristic, average results, ignoring the probabilistic aspect of the process we are studying, we can determine the critical level of SNF (for a given level of the opponent's BMD) at which an aggressor goes unpunished. If, however, we use a different approach, along the lines described in Chapter 3, we will arrive at an opposite conclusion: no BMD system in Alaska or anywhere else, can, in principle, guarantee against retaliation. Why did President Ronald Reagan's Strategic Defense Initiative fail? Simply because an average American voter did not want to believe that such a shield could be 100 percent effective, and rejected the huge expenditures required in favor of other budget priorities. There were other reasons as well, but this one appears to be the main one.

Let us look at the problem from two different perspectives. First, it is impossible to prevent a nation (be it the United States, Russia, or any other nation) from trying to protect itself against various eventualities. Even a very limited BMD system can perhaps somewhat reduce the damage from an external attack. Note the words "somewhat" and "perhaps" – there is no absolute guarantee even here. But the hope, as long as it requires reasonable expenditures, will not hurt anyone. Second, at the same time, the same nation will never give its leaders the right to take a risk, under the cover of such a shield, however highly reliable it is believed to be. The stakes will be too high, higher than at any casino (although the method, sued for risk assessment, is called the Monte Carlo method).

True, it is undeniable that the stronger the BMD of one of the sides, the lower the risk for it. And herein lies the real negative impact of strengthening BMD: Without providing an absolute guarantee, it pushes the nuclear balance to instability, where the risk for a potential aggressor is provocatively low.

The START II level (3,000 to 3,500 of nuclear warheads per side) turned out not to be the lower limit of acceptable reduction. In May 2002, the United States and Russia signed a new strategic arms reduction treaty, which will bring the level of strategic nuclear warheads down to 1,700 to 2,200. It is possible that in reality reasonable redundancy exists around 1,000 or even fewer warheads. There is a feeling, however, that there is a "dead zone" between today's agreements and the realistic redundancy minimum, a gap that the United States and Russia cannot overcome with old methods (that is, blindly). The political opposition will not let this happen and it will be necessary to prove to the nations that it is possible to preserve national security and take such radical steps. To overcome this barrier, mutual research of command and control systems is required. There is no alternative way to disarmament.

Chapter 6

Cooperation

Developing international cooperation between nuclear C^3 experts may be implemented in several stages.

The first stage is a theoretical one. It has two main goals: first, to confirm that a common solution for C^3 problems is not just useful but *necessary*. Second, to convince participants, in the course of joint research using the same models, that stable guarantees of national security for all sides, with a reasonable degree of openness regarding initial data, do indeed exist.

The second stage is to formulate and resolve the most important practical tasks for strengthening negative control of nuclear arms, while simultaneously preserving each party's interest in the area of positive control.

The third stage includes developing joint proposals for a comprehensive consideration of the C^3 factor in the reduction of strategic offensive forces, and in the general process of arms control.

From an organizational point of view, carrying out these stages could result in the creation of an international consultative body for C^3. This body would encourage and monitor nuclear states in the conduct of more rational policies toward command and control, policies that would coincide with the interests of the entire world.

The major characteristic of cooperation between C^3 experts is the inability to develop independently without consideration for the weapons themselves, and without the participation of specialists in operations and general strategy.

It is evident, as noted above, that we cannot evaluate the effectiveness of C^3 without assessing its influence on and contributions to the forecasted outcomes of nuclear operations. In the same way, "pure operators" – that is, experts on weapons and their use – are not able to forecast anything concerning deterrence reliability without a quantitative consideration of the command and control factor.

Therefore, we are talking about the necessity for broader mutual cooperation among experts in various areas of nuclear deterrence, where solutions to C^3 problems would also develop.

At the present time, some international contacts have started developing around separate aspects of global strategic stability, including some between American and Russian military experts. We can mention here the so-called military-to-military contacts program, which includes regular meetings between higher leadership and experts from STRATCOM and the Russian SRF.

The visit of a delegation of Russian experts on strategic missiles, headed by Col. Gen. Sergeyev, to the United States at the end of 1993, was the first such contact. The delegation visited Washington, Offut Air Force Base and Vandenberg Air Force Base. A return visit to Russia by American missile specialists, headed by Adm. Henry G. Chiles, occurred in August-September 1994. Since then, exchanges of expert delegations at various levels have occurred and are continuing now.

It is hard to overestimate the significance of contacts between the missile officers of the two nuclear superpowers for strengthening mutual trust. (At least, American colleagues told Sergeyev in December 1993, in Omaha that "all of them feel very calm while he and his delegation are visiting them.")

Even if we ignore specific serious questions solved in the course of those meetings, the very fact that those people are getting acquainted is extremely important. Further development of the military-to-military program will build the foundation for a subsequent transition to real cooperation between former potential opponents over strengthening strategic stability. Still, joint work has not yet started in many important areas, including topics of command and control. Even when C^3 experts came as members of a delegation, they had nothing concrete to do. Nothing is known about any attempts to conduct joint simulation of nuclear conflicts, even though the necessity for a transition to such cooperation is quite clear.

The first ever visit to the United States by a group of Russian C^3 experts, which took place in August 1997 in California, was a cause for hopes for a breakthrough for U.S.-Russian cooperation in this field. This 10-day visit was informal, although Russian official bodies approved it. This visit was the result of an initiative by Thomas C. Reed, former secretary of the Air Force, and a national security assistant to U.S. President Ronald Reagan, as well as by the author of this book.

The Russian delegation included Maj. Gen. Vladimir Dvorkin, director of the Central Research Institute No. 4 of the Ministry of Defense; his deputy Col. Boris Uchenik; Boris Mikhailov, general director of the Impuls Corp. (St. Petersburg); his deputy, Chief Designer of C^3 systems for the SRF Vladimir Petukhov; General Director of the Central Design Bureau of Heavy Machine Building (Moscow) Aleksandr Leontenkov; his deputy Gleb Vasiliev; and Col. (Ret.) Valery Yarynich. The American institutions represented at the meetings included the Brookings Institution, the Draper Laboratory, the Naval Postgraduate School, TRW and others.

Although these meetings were informal, there was some substantive discussion of common problems of C^3 and of the necessity of cooperation in this field. Two joint proposals resulted from the meetings: one regarding exchange of information concerning organization of negative control in national C^3 systems; the other about establishing a joint monitoring center for control of nuclear proliferation using existing elements of C^3 systems. Although there was no negative official reaction to these meetings on either side, no practical steps have followed.

It appears that the lack of practical results from that first visit originated not only in

the uniqueness of the subject of discussions, but also in the administrative difficulties in Russia, where the government has been overwhelmed by the problems of military reform and social conditions of the Armed Forces. Nevertheless, such meetings were viewed as a precedent for future development of cooperation.

Joint analysis of command and control problems within the framework of military-to-military programs is hampered by the lack of unified theory regarding the place and role of C^3 systems in nuclear forces, and the absence of a clear and unclassified methodology for the quantitative assessment of its contribution to deterrence. The most important obstacle here is lack of clarity regarding guarantees of national security when working jointly in such a sensitive area. It seems that without joint theoretical work on the question of guarantees, a discussion of practical goals concerning C^3 will never begin. And without that, serious talks about assessing the reliability of mutual deterrence or perspectives for reducing nuclear arsenals are impossible.

Notably, the difficulty with "guarantees" predetermines two main conditions for overcoming it successfully: first, this work is to be done jointly by American and Russian experts on a unified theoretical basis; and second, the openness of such work is mandatory. The first condition proceeds logically from previous conclusions. A lot has been said about openness, but it is crucial to add that no matter what results such work will bring, it should not remain hidden from the world community. This is not an internal affair for the political and military leaders, since it involves the interests of their nations, as well as other nations.

To stop fearing the unknown, to prevent going to extremes because of these fears, to come out with reasonable estimates of how and to what level to disarm, to give the world a guarantee against nuclear war, only one thing is needed: *This war needs to be conducted.* One hundred thousand times, using a unified model.

First, the sides will convince themselves and each other (the latter is even more important) that it is impossible to reduce the risk (to the aggressor) to zero in principle. This will serve as joint theoretical proof of the senselessness of nuclear war.

Second, everyone will see, if even tentatively, the quantitative levels of deterrence. From here various scenarios are possible for further activities.

If the results show serious superiority and not particularly robust deterrence for one of the sides, it is bad for everyone. In this case, something will have to be done to increase stability: either to stop arms reductions, or urgently develop some elements of forces, or even provide help to the "defeated" side from the "victorious" one. At that, no one will be able to blame the weaker (or "less strong") side for its activities since it will be clear that they are in everyone's interests.

It is not, however, impossible that the results obtained in the course of joint work by scholars and military experts will be acceptable to the public, for both sides and for world stability. There are no guarantees that at this point nuclear professionals in the United States and Russia are not "stuck" on very high levels of deterrence – the exchange of hundreds or thousands of nuclear strikes. (Many experts, including Ameri-

can experts, think that nuclear deterrents of France or China are quite sufficient.)

Briefly speaking, an optimistic assessment will allow to plan and implement measures for a gradual reduction of nuclear arsenals and their readiness, transition to safer concepts for peacetime, and doing it all in the most conscious and open way. Consequently, no one in the nuclear states will be able to blame their leaderships for "lack of patriotism" and prevent important, reasonable steps for strengthening strategic stability. Today, such reasonable behavior in the United States and Russia sounds like Utopia. And yet, we should strive to achieve such a level of public consciousness. It is no longer possible for the two teams to play with fire on a huge barrel of gun powder without any rules while the cover of the barrel is gradually rotting. It is better to work out those rules. It is possible to do that in stages.

Suggested stages of cooperation follow.

6.1 The Stage of Theory

Even now, it is possible to get together a small group of independent American and Russian C^3 experts and "pure operators," and ask them to develop a theoretical foundation for further cooperation in two main directions: negative and positive control.

No special theoretical proofs regarding the usefulness of cooperation over negative control are required. The only important goal here would be proving that during the exchange of technologies for protecting nuclear weapons and C^3 from accidental and unauthorized use the sides would not, "along the way," touch upon those other parts of the C^3 structure that are relevant not for protection from unsanctioned actions but rather belong to the sphere of positive control, for which it is much harder to reach mutual understanding. Still, this is not a serious obstacle, and it is rather simple to create and agree on a protective barrier against an initially undesirable mixing of the two issues.

Theoretical tasks would be more challenging for positive control. We can recommend the following schedule for contacts between C^3 experts in this area:

a) Develop or choose, from those available, a statistical simulation model and methodology for researching the influence of command and control systems on the assessment of mutual nuclear deterrence; for example, the scenario described in Chapter 3;

b) Agree on a set of conditional initial data for the C^3 of both countries. Those will include already known (unclassified) information on the structure of the systems, their fixed components, the standard physical parameters of communication channels, etc. Each side would be able to include any number of conditional elements and characteristics in this set for insurance;

c) To study, by simulating a hypothetical nuclear conflict, changes in the parameters of a retaliation strike under different scenarios with the following initial data:

- strategic groupings of the victim's nuclear forces (those are the weapons that are almost completely declassified by both sides);
- "conditional" command and control systems for these groupings;
- concepts of retaliatory actions by the victim (LOW, LUA, DSS);
- means and strategies of the aggressor's attack (also declassified to a consider able degree at this time).

d) Draw, based on the above, conclusions regarding two main questions: first, does a limit for reducing the risk to the potential aggressor exist under any increase in the aggressor's initial military and technical superiority over the victim? Second, to approximately which quantitative level of parameters for retaliation (magnitude of the strike and its probability) does this limit correspond?

In other words, the goal for the first stage of joint research on positive control should be to find a scientific foundation for the guarantee of a nation's strategic security under any conditions, and to prove the senselessness of initiating nuclear war against it, in principle.

Most people intuitively feel the existence of solid guarantees against initiation of a nuclear war in view of its special character. It would be possible to avoid proving theoretically such guarantees. But in a situation where some arms are reduced and others developed, it is desirable to know the level and price of those guarantees.

The level of "minimal" risk for the aggressor obtained as a result of joint theoretical work might, indeed, seem not too large in absolute terms. Let us assume, just for example, that it would be about $P(N \geq 50) = 0.3\text{-}0.4$. This means that in spite of the aggressor's very high preparatory efforts, he has no guarantee against retaliation. The risk looks like this: the potential victim is able to deliver the minimum of 50 nuclear warheads on the territory of the aggressor state with a probability of 0.3-0.4. And the targets (any can be hit) are not known in advance.

Take the example of another "lowest" risk: $P(N \geq 20) = 0.6\text{-}0.8$. Is this high or low? C^3 experts should not give an answer to this question: it is not their business. They will just show what they have as a result of modeling. But everyone should take part in making assessments and taking decisions on the sufficiency of the guarantees for reliable deterrence. The decision should be made in a democratic way.

The idea of this approach is that, instead of some abstract, average values of risk, even the least probable – but nevertheless catastrophic – results of nuclear simulations would be revealed and assessed. It is unacceptable to ignore even the most extreme results of simulation (the way it is usually done in statistical research).

To achieve an accurate enough assessment of extreme scenarios, a rather large statistical sampling is required – that is, a lot of simulations per each scenario. This is not a problem for modern computers. At first glance, the most difficult task is agreeing on initial data for the probability characteristics of C^3 systems, such as survivability of nodes, reliability of communication channels, etc. In reality, however, there is no need

to look for anything new here: this approach uses the same initial data as all other methods now used by military and research institutions of various countries. The difference lies only in the choice of presenting the simulation output's final results.

As for the concepts of "a little" and "a lot" as related to nuclear deterrence, this was already discussed in previous chapters. We can quote some more from American civilian and military experts: "... because Robert Jervis believes that Soviet leaders are aware of the extremely high costs of nuclear war, he judges that even a small probability of such a war is sufficient to deter Soviet leaders." This underlies his response that "the argument that the American threat to use nuclear weapons is not very credible glosses over the point that only a little credibility be required."[263]

Bernard Brodie presents a similar position: "It is a curiosity of our times that one of the foremost factors making deterrence really work and work well is the lurking fear that in some massive confrontation crisis might fall. Under these circumstances one does not tempt fate."[264]

Harold Brown argues that "... Even when the probability of an event seems low, it may (depending on how costly the effort) be worth reducing still further when the consequences of its occurrence are so great."[265]

In 1992, Frank von Hippel, a well-known American expert, was familiarized in Moscow with the assessment method described here, and was asked what level of risk he considers (conditionally) acceptable even to consider a surprise attack against Russia. Without any hesitation, he wrote: $P(N \geq 1) = 0.00...1$(!) Many would find this kind of risk a bit low but this answer is symbolic in many respects.

In the spring of the same year, I was going home by train in the same compartment with a Russian nuclear physicist who had worked with Andrei Sakharov. He was trying to convince me that, from a purely scientific point of view, 200 to 300 nuclear detonations on the territory of a country such as Russia or the United States would not bring devastating consequences to those countries, and even less to the whole planet. He found any comparisons with Chernobyl "inappropriate" since "this is a totally different matter." I could not argue with this highly skilled professional in his terms. I did say, though, that even if he was theoretically correct, he would never be able to convince the majority of civilians, simply because they will not want to believe him. My opponent could not argue against such a "non-scientific" argument.

The prospect of nuclear war is almost unacceptable for a human being. This is a solid guarantee, and a basis for the "workability" of the suggested approach for assessing sufficient levels of deterrence.

Assessment of results obtained by a group of C³ experts in the course of suggested research may bring about various subsequent activities. If they conclude that calculated values of "minimal risk level" do not satisfy requirements of reliable deterrence, each side will have the right not to declassify in full their connectivity graphs. Both partners can also leave the situation in the same uncertainty that they have today, stating they have a number of additional real C³ elements that they did not include earlier

in the considered joint "conditional" simulation model.

There is hope though, that the results of such joint theoretical research will bring more beneficial results.

In 1990-1992, some assessments using this method were carried out at the Center for Operational and Strategic Research of the Russian General Staff. The results were reported to the Ministry of Defense. Although the work was formally approved, there are no indications that its results had any impact on the work of the military industrial complex. Nonetheless, some of those conclusions are worth mentioning.

First, the unclassified report dealt with theoretical issues, and included a suggestion that there is, indeed, a bottom threshold for risk reduction to the potential aggressor, although the potential quantitative level was not established since the research was unilateral (no U.S. experts participated). Second, the report concluded that in the early 1990s, given the existing weapons on both sides and real characteristics of the Russian nuclear C^3, the probability of Russia retaliating against the United States with no less than 800 to 900 nuclear warheads was 0.6-0.8. Another conclusion suggested that, even with a considerable increase in the aggressor's nuclear forces (compared with the data used in modeling), and with the most unlikely American perceptions of acceptable damage, the value of the indicator of deterrence $P(N \geq N_{given})$ would be more than sufficient to prevent a nuclear attack against Russia.

At the same time the work demonstrated that should the process of reducing nuclear forces on one side and developing offensive forces by the other continue, the level of risk to the aggressor would decrease. If no measures are taken to improve command and control systems, by 2003 the following indicators may be expected: $P(N \geq 200) = 0.3$ or $P(N \geq 100) = 0.5$ or $P(N \geq 50) = 0.6$. A question was raised: At what level a deterrence indicator should be maintained to achieve guaranteed deterrence, and how to achieve that level? The report then listed various scenarios for achieving this goal, with approximate financial estimates.

That work was one of the first attempts to approach the problem of deterrence from a new point of view. For obvious reasons, it was unilateral and, therefore, may not be considered as the beginning of joint theoretical research. But the method that was used could be employed in joint research.

If the theoretical stage of cooperation confirms the existence of reliable and redundant guarantees for both sides, along with mutual deterrence, official institutions can give a "green light" to the subsequent practical stage of joint work.

6.2 Initial Practical Steps

The parties, safeguarded by a mutually proved guarantee of security, may start to develop and implement the most important measures in the C^3 area, the goal of which will be strengthening strategic stability. The main emphasis should be on increasing negative control. Metaphorically speaking, the security of nuclear weapons and command and control systems from accidents and sabotage will be increased in practice,

while the ability of each side to punish the aggressor (that is, positive control) will be gradually transferred from everyday life to the domain of paper and modeling. With that, there would not be even the slightest reduction in the real effectiveness of nuclear deterrence, proved during joint theoretical work for all alternatives. The ability to retaliate will be "locked in a box" (or a fist hidden in a pocket, if some prefer this comparison). The danger of a tragic slide toward nuclear war is reduced.

It would be useful to start the organizational stage of the second step with each side's official confirmation of a data list for national C^3 systems in the areas where unclassified publications and joint research are allowed. The bilateral expert group may prepare such a list on the basis of the theoretical stage of the work.

Here is an example of a list:

Issues of Nuclear Command and Control for which Joint Research and Unclassified Publications are Allowed or Banned

Open Constant Group

These are topics on which cooperation may be allowed even prior to conducting the joint theoretical research. They are questions that are relatively permanent:

- composition of C^3 system, and real names of its main structural elements that are in operation;
- general principles and elements of the system's architecture and operation;
- locations of stationary command posts, operational large transmitting centers and satellite communications centers;
- design bureaus and research institutes of the Ministry of Defense, and industries, enterprises and institutions involved in development and mass production for C^3 as a whole and its components. This includes names, locations, names of commanders, history of creation and development, main responsibilities in C^3;
- design operating principles and reliability of C^3 protection systems against accidental or unauthorized launch of nuclear missiles; the same for components of the system and blocking code devices at all levels of command and control (this would be open only to the experts, while only their conclusions would be published);
- concepts for combat use of C^3 in hypothetical nuclear conflict scenarios, instructions on actions of national leaderships and duty crews at command posts of all levels in a critical situation, the system of predelegation from the commander in chief down to the lowest levels; available scenarios of autonomous missile launches;
- methods used for evaluating C^3 according to the cost-effectiveness criteria under general SNF evaluation; corresponding models.

Open Extra Group

This includes additional information to be released after conducting theoretical research

and creating a joint assessment method for the effectiveness of mutual deterrence from the C³ standpoint:

- the actual current number of elements in command and control systems. It would be useful to give the parties the right to declassify only that part of the information sufficient for achieving the calculated goal of confirming mutual deterrence. The rest of the data would be better off classified, to maintain reliability.

Ban Probable Group

This includes banned questions of variable nature that might serve as probability characteristics for the opposing side:

- real values of launching codes, blocking codes, key data for the encrypting equipment;
- working radio frequencies, passwords and communication session schedules;
- locations of field positions for mobile land-based elements of the system, redundant (concealed) airports for airborne command post (ACP), schedules for the mentioned C³ elements moving into those;
- development of new, prospective systems of C³ (prior to starting their operation);
- plans for combat employment of nuclear missiles with a list of their targets.

A similar list will be elaborated and supplemented according to the results of the work's first stage; that is, theoretical calculations based on a unified simulating model system.

Upon agreeing on the list of open data for command and control systems, Russia and the United States might conduct a series of expanded work meetings among experts to discuss some initial practical steps. It would be helpful to first hold a special seminar in order to formulate specific tasks for work groups, create those groups, and resolve organizational and financial questions.

Including specialists with different areas of expertise related to C³ in such work groups is an important condition for success:

> "It's crucial, therefore, that the small group making up the 'C³ community' today be expanded to include more than a few engineers, behavioral scientists, communications specialists, defense contractors, and military people. ... Limited inputs, though, can lead to narrow thinking, and C³ issues are too important to be left to a few self-designated experts."[266]

From experience we know that those experts understand each other very well during such meetings:

> "Fundamental to understanding C^3I ... is to know who you're talking to. If he is a technocrat you can talk to him in terms of a 'C^3 system.' If, on the other hand, you're talking to a manager ... you'd best talk about C^3I, because you're talking about a program - a chunk of the Department of Defense Budget. If you're talking to an operator ... then you're talking about a process, a command and control process, which is facilitated by a program. ... They have a differing perspective on what it is you're talking about when you say command and control."[267]

The work described here may be done both on the official level under the auspices of the governments, or independently, with the cooperation of international organizations and funds. In any case, the Russian and American official structures should simultaneously prepare corresponding agencies that would receive any recommendations from these expert groups and implement them.

During their initial meetings, C^3 experts, while getting acquainted, might review possible ways to resolve the following tasks:

a) Agreeing on one standard for keeping nuclear weapons safe from accidents and unsanctioned activities. The parties should use their best achievements in this area, develop the best organizational system from top to bottom, make efforts to eliminate weaknesses and implement modern technological methods, etc.

   Should standards be agreed upon, it would be possible to check national weapons and C^3 systems for satisfying these requirements. Systems found lacking would then be improved. Systems found not worth improving should be removed from combat duty and be the first ones eliminated. Mutual assistance, including ideas, funds, technology and specialists, would not be out of the question at this point.

   After close cooperation is established in this area, it would be useful to attempt spreading positive experience to other nuclear states, including China. The ability to secure nuclear weapons and command and control systems of undeclared nuclear states may be achieved with the same approach.

b) Jointly developing special technical systems able to react quickly during potential terrorist seizures of nuclear weapons. Such systems should provide immediate information on seizures to leadership, as well as potentially transmit orders by radio and satellite directly to technical devices that would automatically block the weapon(s) or eliminate it in an ecologically acceptable manner. These systems should be capable of being used exclusively by the country possessing the seized nuclear weapons.

c) Eliminating the traditional peacetime predelegation of nuclear responsibilities from the national command to lower levels (including the elimination and changing of encrypting codes given out earlier).

d) Confirming, using joint simulation with real (unclassified) initial data, actual and reliable mutual deterrence within LUA (DSS); agreeing on the sufficiency of the deterrence indicator's calculated values, taking into consideration prospects for arms reductions, prognoses for military and technical progress, and deep reductions in levels of nuclear readiness.

e) Implementing, upon those agreements, the following measures:
- official rejection of LOW as the primary concept; removing from the command posts instructions on conducting immediate retaliatory strikes in response to information from the EWS of a nuclear attack;
- taking more decisive steps to decrease combat readiness of nuclear forces, including undocking warheads from missiles. Here most of the suggestions described by Blair and other American authors within the framework of zero alert may be used;
- agreeing on acceptable measures for increasing the readiness of command and control systems for a retaliatory strike if necessary; developing clear, accurate external signs that would distinguish between those measures and the activities in preparation for a first (pre-emptive) strike;
- involving observers from other countries in staff exercises of command and control systems; practical demonstration of C^3 capabilities for those observers, including the functions of separate elements providing for the effectiveness of the LUA (DSS) posture;
- simultaneous introduction into national legislation of limitations on production and acquisition of potential countermeasures to nuclear command and control systems.

There is no doubt that positive achievements of the experts' joint work will expand this initial list.

Let us emphasize again that implementing the measures for strengthening negative control (points a, b, c, and similar measures) may be carried out independently of any steps for maintaining positive control at the required level (points d, e, and similar). Implementing some of the suggestions will only require the parties' agreements and corresponding directives, while others will require the development and implementation of corresponding technological equipment.

6.3 Prospective Trends in Mutual Control

Successful work on the second stage of cooperation will bring us to creation of a permanent international C^3 expert organization, the existence of which seems crucial.

First, common internationally legalized "rules of the game" should exist in nuclear command and control as they do in communication, navigation, ecology, etc. The threatening character of potential violations of C^3 "rules" makes permanent control over their

implementation, particularly by the nuclear states, absolutely necessary.

Second, an international C^3 agency could become one of the main sources of scientifically proven recommendations for choosing the most rational development for nuclear command and control systems. Its participation in analyzing the potentials, volumes and pace for deep nuclear arms reductions would also be a valid aspect of its work.

Third, a broader structure in charge of controlling the EWS (C^3I), military computers sphere (C^4I), etc. may be created later on the basis of such a C^3 body.

Finally, the international character of such an institution would allow for provision of the financial means necessary to implement major, long-term and costly programs in the area. Those programs may include:

a) Creation of accurate, standardized systems for detecting nuclear attack, with the goal of providing those systems to all nuclear states.

b) Developing and implementing technology to reduce the consequences of accidental or unauthorized launches of nuclear missiles; improving weapons and command and control systems already in existence; in this respect, Sherman Frankel's ideas may be used.[268]

c) Creating a special unified, automated communication and control system for nuclear weapons, in addition to the telephone and telex "hot lines" already operating between the heads of the nuclear states, as well as between the national centers for reducing nuclear danger.

d) Ongoing refinement of methods for calculating the C^3 factor into agreements on deep reductions of nuclear weapons. On this basis, minimization of general expenses for maintaining a reasonably sufficient level of mutual deterrence.

e) Regular publication of bilateral White Book on the problems of nuclear command and control.

f) Developing a theoretical basis for the place and role of nuclear C^3 within broader strategic stability, and subsequent creation of a minimal standard for national C^3 systems, providing for their stabilizing character.

g) Developing control over the C^3 activities of the "unofficial" nuclear states, and rendering help, if necessary, to improving their command and control systems to the required standard level.

At this point it is impossible to predict how actively, and in precisely what directions, cooperation may develop. But it is clear that this would encourage the strength-

ening of global strategic stability. Cooperation over C^3 has to start with the first, theoretical stage, without which a transition to practical measures would be most difficult.

6.4 If We Do Nothing ...

What would happen if not a single proposal listed above were implemented? What would happen if we continue to ignore the potential dangers of nuclear command and control, including both positive and negative control?

Any study claiming to be objective assumes an analysis of all possible alternatives, including the worst and the least probable ones. When dealing with nuclear deterrence, this requirement is especially relevant. Since the fate of civilization is at stake, the sides have to study all possible outcomes of nuclear deterrence, however fantastic and unpleasant they could be. They must see these nightmare scenarios to the end, so that in real life we could make the right conclusions and take these scenarios into consideration.

Let us consider only some of the hypothetical situations that we might face in the future, and try to forecast the course of events. First, let us consider the issue of positive control: is it strong enough to prevent deterrence from deteriorating into a real test of strength?

The world has changed significantly since the Cold War. It is difficult to imagine that Russia and the United States would return to the level of mutual ignorance and suspicion that characterized their relationship in the 1950s to 1970s. Nevertheless, even today there are many potential causes for deterioration of relations.

In an imaginative scenario, all peaceful means for resolving a political crisis have been exhausted, and the West and Russia are on the brink of war. Prior to the crisis, while the relations were good, both sides implemented deep reductions of nuclear readiness. But, unfortunately, the time buffer provided by the reduction of readiness has not helped both sides to reach an agreement, and now they have returned to a dangerous hair trigger posture, in which missiles are ready to launch in a few minutes.

Because of the complete lack of information about command and control, and the absence of joint U.S.-Russian assessment of a possible conflict's results, the military staffs of the United States, NATO and Russia have prepared military options and are now ready to implement them. The less informed about one another, the crazier are the plans. Let us assume that the Pentagon, ignorant about the real capabilities of Russian C^3, thinks that they can swiftly decapitate and suppress the Russian C^3 system. This could be attempted, for instance, by a simultaneous strike through the "holes" in the EWS against the key nodes of the C^3 system, several high altitude blasts of super-EMP weapons, massive radio interference across all wave bands, sabotage on Russian territory, possibly with seizure of several command posts, etc. The concrete details of such a plan are not that important; rather, it is dangerous that such a plan exists and by itself promotes its execution. (One may remember here Anton Checkhov's observation about theater: if a gun is seen hanging on the wall in Act One, by the end of the play it must shoot.)

Military operations, including those using conventional weapons, have not started yet, but the sides are in a state of unstable balance and uncertainty, which we remember from the Cuban missile crisis. Each side fears the other's preemption. In this situation Russia, aware of the West's fears and of its operational plans, may take various courses of action. First, it can wait without upsetting the fragile balance; but this choice appears dangerous because Russia lacks a reliable assessment of its capability to retaliate if attacked first. If the Russian leadership has such an assessment, it is not particularly dependable because it is unilateral, and, most importantly, the potential aggressor is not aware of this assessment. The second possible course of action for Russia is to carry out a pre-emptive strike, now coordinated with the official military doctrine; but even selective strikes by TNW will inevitably lead to a global escalation and catastrophe. Finally, the third option would be to delegate, at the last possible moment, nuclear release authority to various lower levels of the command and control system. This, however, increases the danger of war because of an accidental (or unauthorized) action by at least one of the command posts that receive nuclear release authority and all necessary codes. As noted earlier, it is technically impossible to remove the potential for predelegation, and it should not be done: with this potential built into the system, any attempt to decapitate it would be tantamount to putting out fire with gasoline.

The conclusion from nightmare number 1 is obvious: all operational plans of attacks against opponent's C^3 systems should be removed from all command posts, declared unrealistic and dangerous. Once joint assessments of possible outcomes of such attempts are conducted, we will obtain reasons not to make such attempts: retaliation is possible, global ecological consequences are catastrophic, etc.

Nightmare number 2: Immediate launch of missiles in response to false information from the EWS. This "classical" mistake has been well investigated and is widely described in many unclassified studies. This book has also addressed the issue, so I will only mention some conclusions. First, it would be useful to organize a constant presence at all C^3 facilities of representatives of other members of the nuclear club, probably as well as of international organizations. These representatives should be present not only at EWS centers, as is already being done to a certain extent by the United States and Russia, but also directly at the central command posts of nuclear forces. Of course, this cannot completely exclude the possibility of unpredictable actions by one of the sides in a critical moment. Therefore, it will be very important for the United States and Russia to reject LOW as the main posture, and to replace it with LUA. Thus, as I said earlier, operational documents at command posts should contain references to LUA rather than to LOW. This more than 40-year-old delusion must be corrected at last, if for no other reason than because no one really knows how humans will behave in such a super-unique situation, at a threshold of war. The Cuban missile crisis teaches us little in this respect, since EWS did not exist then. One should not stake everything on a completely unpredictable phenomenon without any results of real life experiments, without any concrete knowledge – which cannot be obtained.

Joint research and assessments will help explain why LUA can become the main posture.

Now I would like to address some possible (although highly undesirable) scenarios of development of events in the field of negative control: are C^3 systems reliably protected from accidents and unauthorized actions?

International crises test negative control as well as positive control. A missile launch as a result of an EWS error is a complete failure of negative control. Similarly, negative control disintegrates after predelegation of nuclear release authority down the hierarchy of command and control: even if the crisis is over, the compromised C^3 codes may be, for some time until they are completely replaced, used for unauthorized actions.

Today the greatest problem is the possibility of serious weakening of negative control in peacetime. The situation in the world does not favor reliable protection in this field and is deteriorating. There are more than enough reasons for concern: international and domestic terrorism; smart computer hackers, some of whom may be interested in more than practical jokes; discontent among personnel with access to C^3 systems; deficiencies of certain systems, as well as their obsolescence; and finally, a possibility of a mentally ill person in a position of considerable power.

It would be wrong to analyze here in detail various scenarios of such potential threats; such an analysis could serve as a textbook for terrorists. (One should say here that designers of negative control systems should model all thinkable and unthinkable actions by an intruder.) For instance, here are some general hypothetical scenarios.

- In (for instance) France, a group of Arab terrorists has seized an SSBN. They find out (either while already on board, or in advance) the secret of launching SLBMs. The terrorists begin to blackmail the world, and, to confirm their seriousness, they launch one SLBM, which detonates with a warhead(s) somewhere in the ocean. If, however, they do not possess the secret of negative control, they still bluff that they can launch their SLBMs. Finally, when an attempt to eliminate the terrorists is mounted, they blow up the whole SSBN, with all attendant consequences. Or even worse: they manage to launch one or more SLBM – but this time against land-based, real targets.

- A teenage hacker anywhere in the world studies the structure and operations of an important element of the U.S. strategic C^3 system. (Since this system is relatively well connected with wider computer networks, this is possible in principle. At least, there have already been intrusions into military networks.) Then, the young hacker announces via the Internet that he has created a virus capable of blocking the work of these U.S. C^3 elements. In order to demonstrate how well versed he is in the subject, the hacker explains some technical details that C^3 experts can understand. He says that he can launch the virus before he is caught. The teenager also mentions how long it would take to eliminate the virus and unblock the C^3 system. This will serve as food for thought to other countries as well.

- In one of the Russian ICBM regiments, a captain from the duty crew, driven to distraction by lack of housing, miserly pay (which also is sometimes delayed), family problems and lack of confidence in his and his family's future, has gone completely mad: he informs the mass media that during his time in underground command posts he has discovered the code blocking the combat launch equipment. Further, he says that he has shared the information with several of his colleagues in other military units (the code is common), and that they can, in principle, launch the ICBMs on their own, although only at targets already in their computer memory. (The captain knows very well that today's detargeting is nothing more than a show.) Of course, this is only a bluff: the captain never shared any information with anybody, because he could not possibly break the code. But only Russian experts understand this. In view of world reaction to this episode, the Russian military command has to completely replace the code throughout the entire nuclear forces – an extremely problematic act.

- One of the old Russian regimental command posts, which controls 10 remote autonomous ICBM silos, loses all communications with the outside world – and with its own launchers – for several hours, because of a breakdown of the worn-out equipment. The regiment, which always kept live communication links, completely disappears from the sphere of negative control. One can imagine the feelings of the higher command, which does not know why the regiment has "disappeared," and is justifiably concerned over the fate of the regiment's people and missiles. This would be bad enough if the episode takes place in peacetime; but what if it happens during an international crisis?

- In Pakistan and India, less than responsible politicians have come to power, another crisis over Kashmir has flared up, there is fighting – so far – without nuclear weapons. Unfortunately, because of a failure in the maintaining system of the command and control system, a nuclear explosion occurs. This is confused with an attack, with an "adequate" retaliation following and subsequent escalation. This turn of events has negative consequences not only for the two nations, but also lowers the nuclear threshold in other troubled regions.

The number of such hypothetical situations is large enough, and is growing. It would be wrong to limit our concerns over negative control only to Russia. Russia has its problems, but so do other nuclear nations.

The problem of negative control is objective for all nuclear nations, and it can be solved only at the global level with the cooperation of all interested parties. Unilateral actions in this area, even if they are 100 percent effective, cannot prevent attempts to test the strength of command and control safety systems. The problem is the degree of trust in unilateral declarations. A terrorist may believe declarations by one nation that

its C^3 system is completely secure – or he may not believe it. But affirmation of security of C^3 systems coming simultaneously from U.S. and Russian officials is much more impressive and more likely to dissuade anyone from testing the system. Neither the United States nor Russia would gain anything from covering up the other side's deficiencies, since it is in the interest of both that the other's negative control mechanism is in order. In such case, the public will be much more likely to trust the experts, who say that the terrorists, the hackers or the unfortunate Russian captain are only bluffing.

As for an insane leader at the top of a C^3 pyramid, one hopes that this will not happen, that the leaders of all nuclear states will be rational, at least rational enough to cooperate in C^3. As a first step, the United States and Russia could share with each other the lists of possible intrusion scenarios that are modeled on both sides of the Atlantic when developing systems of negative command and control.

Conclusion

It is probably true that the main outcome of the Cold War was not only the "victory" of the United States over the Soviet Union, and of the West over the East. In the final analysis, all nations have benefited from the disintegration of the Soviet empire and the Socialist camp. An equally important outcome is that the 40-year long global political and military confrontation ended peacefully without a nuclear catastrophe.

Nuclear weapons should not be viewed as a political instrument. Nevertheless, Margaret Thatcher, the "iron lady," was right: nuclear weapons have kept peace on earth for decades. A hypothetical aggressor is deterred from the temptation to use the nuclear trump card not so much by fantastic scenarios of nuclear war and retaliatory strikes developed by the opponent (the potential aggressor could only guess about the content of such plans), but by the mere existence of the opponent's nuclear arsenal. The political leaders and military officers who have access to the nuclear "button" naturally fear unpredictable global consequences. This fear is the most reliable guarantee of peace.

It is insufficient, however, to pay attention only to the obvious qualitative aspect of nuclear deterrence. It is equally useful to view the quantitative aspect of this question and track the changing positions of politicians and military commanders regarding the sufficiency of nuclear deterrence. The evolution of these views during the Cold War demonstrated that the invisible nuclear threshold is a very relative thing. Without going into detail, let us take note of two extreme points: in the 1970s and 1980s, both the United States and the Soviet Union believed that 10,000 to 12,000 strategic nuclear warheads for each side were barely enough to preserve strategic balance, even under the limitations on BMD imposed by the 1972 ABM Treaty. And now, Russia and the United States are ready to reduce their nuclear arsenals down to 1,700 to 2,200 strategic warheads, while work on NMD is unfolding in the United States. Why such a drastic difference?

It appears that the intuition of the two nuclear superpowers' leaders has turned out to be better than the complicated calculations of their military strategists. George W. Bush and Vladimir Putin have actually shifted to a new kind of logic, and the General Staff and Pentagon must be drastically reviewing their operational plans to correspond to new, more rational political attitudes. It is becoming increasingly clear that the old scenarios of nuclear war and the respective requirements to the structure and composition of nuclear forces were developed using erroneous methodologies. Initially, both sides relied on the simplest principle of approximate equality of arsenals, which is by

no means a scientific approach. Then the approach was correctly complemented by assessments of the possible magnitude of retaliation; but these assessments were based on the most probable (average) outcomes of war simulations, which is a serious methodological error. Even if retaliation by a victim of aggression is not highly probable, it may still have catastrophic consequences for an attacker, something that a "rational potential aggressor" cannot discount. Since catastrophic consequences of retaliation are possible in principle, as demonstrated by numerous simulations of a hypothetical conflict, deterrence would be reliable even when nuclear arsenals are rather small and a BMD system is deployed.

Nuclear planners ignored this obvious fact for many years, and their delusion exacted a huge price from both the Americans and Soviets. After wasting vast resources, both sides are now rapidly moving toward reasonable, sufficient levels of nuclear arsenals. The politicians have taken a correct and courageous decision, but now we are facing a certain methodological vacuum: it appears that neither side can convincingly substantiate this decision. If appropriate substantiations exist they should be revealed, and the public in both countries will be reassured. So far this has not been done.

Common sense is good, but sometimes it's not enough. Russia's calm official reaction to the U.S. decision to abandon the ABM Treaty was immediately followed by the Moscow Treaty of May 2002 on radical reductions of nuclear weapons. Until recently, the combination of such two actions would have been viewed as complete nonsense. Why has it turned out, after all, to make sense?

As long as there is no clear answer to this question, which is hardly rhetorical, there will be stubborn resistance from the opposition to this sensible course of action, which is approved by the majority of people both in Russian and the United States. This resistance may grow in response to further advances in arms reductions. It will have a negative impact on the domestic politics of both nations, and even drag us back to the thinking and actions of the Cold War era, with resulting challenges, conflicts and expenditures.

This book proposes a possible approach to the joint U.S.-Russian substantiation of sufficient level of nuclear deterrence. This approach employs the system of command and control. Without reasonable openness in this area and correct accounting for the C^3 factor, it is hardly possible to begin to rely upon such an informative indicator of deterrence as "probability of retaliation not lower than required." And without this indicator, it is practically impossible to evaluate the "unlikely" but catastrophic outcomes of retaliation, which are the real deterring factor. The approach proposed in this book fits the logic of common sense, with the new thinking of politicians who have cut the Gordian knot of offensive strategic weapons and BMD. This approach can serve as a basis for developing a theoretical foundation for current and future political decisions in this area.

The theoretical aspect of our approach is quite simple, and most probably will not provoke serious objections. Practical implementation of this approach, however, is

much more complicated. Experts working on implementation of this approach will have to explain its advantages to their leaders (users) – a difficult task. It will be necessary to overcome the barrier of mutual distrust between the recent adversaries and begin to cooperate in the secret field of C^3. Joint U.S.-Russian modeling will run into the problem of initial data because of secrecy. But, as this book demonstrates, this problem could be resolved. Finally, after the results of joint modeling are obtained, we will always face the problem of choice: how much is enough for reliable deterrence?

One can name more obstacles toward implementation of this approach. But one can hope that all these doubts result not from any shortcomings of the proposed methodology, but rather from its novelty. After all, we are proposing a qualitative shift from an abstract fear of retaliation to a quantitative measurement of its probability and magnitude. Initially this measurement will be approximate, but subsequently it will become more precise and detailed. Our approach also provides for estimates of expenditures for each scenario. Thus, improving the system for assessment of deterrence will save billions of dollars – as well as provide more certainty.

Joint work by U.S. and Russian experts can also bring other benefits, such as convincing each side that its national security will not suffer in the process of exchanging data on nuclear C^3. This conclusion and exchange of firm guarantees of deterrence would allow both sides to cooperate in the crucial protection of nuclear C^3 systems from unauthorized actions. Today, under conditions of global war against terrorism, this mission is paramount.

The book proposes cooperation in the area of C^3. Where to begin? Much has been said on this subject throughout the book. Suffice it to say that an open wide-ranging discussion of the approach proposed here is the first priority. Perhaps someone would offer a more attractive alternative leading to the same goal: substantiation of minimum sufficient levels of nuclear deterrence and development of U.S.-Russian cooperation over nuclear C^3.

If this happens, this book has fulfilled its mission.

Appendix 1

1. Yarynich V.E. "Military Thought" (Voennaya Misl'), Moscow, N 12-1990 and N 9-1991.
2. Yarynich V.E. "Ways to Security," Peace Research Institute, N 3/9, 1992, Moscow, pp.39-52.
3. Yarynich V.E. "Influence of Command Systems (C3I) on Strategic Stability Estimation." "Implications of the Dissolution of the Soviet Union for Accidental/Inadvertent Use of Weapons of Mass Destruction," International Conference, Piarnu, Estonia, April 23-25, 1992. Published in Tallinn, pp. 213-221.
4. Yarynich V.E. "Brains or Muscles?" "Towards a Nuclear-Weapon-Free World," International Conference "Swedish Initiative for the Prevention of Nuclear Proliferation Risks and New Nuclear Threats," Stockholm, Nov. 19-21, 1992. Published in Stockholm, 1993, pp. 155-159.
5. Yarynich V.E. "New Times" (Novoe Vremja) NN 10 and 33, 1992.
6. Army Gen. Maksimov Y.P., ed. Raketnye voyska strategicheskogo naznachenija, Moscow, 1992, pp. 81-83, 123-126, 156-157.
7. Yarynich V.E. Allgemeine Schweizerische Militarzeitschrift, Nr.4, April 1993, p.153-155.
8. Yarynich V.E. "About command system's role and place" (in Russian). "START-2 and national security of Russia," CGMF, 1993, pp 24-34.
9. Sutyagin Igor. The Use of Force, Nuclear Weapons, and Civil-Military Relations in the Soviet Union and Russia. "Civil- Military Relations and Nuclear Weapons." Center for International Security and Arms Control, Stanford University, June 1994, pp.111- 138.
10. Podvig P.L., "The Operational Status of the Russian Space-Based Early Warning System," "Science and Global Security," 1994, Volume 4, pp. 363-384.
11. Khronika osnovnykh sobytiy istorii RVSN (k 35-letiyu RVSN), Moscow, 1994.
12. Veterany-raketchiki vspominayut (k 35-letiyu RVSN), Moscow, 1994.
13. Yarynich V.E. "Yadernye strategii i faktor upravleniya," Segodnya, March 30, 1994.
14. Yarynich V.E. "The Doomsday Machine's Safety Catch." *The New York Times*, Feb. 1, 1994, p. A17.
15. Yarynich V.E. Otsenka garantii, MGIMO, Moscow, 1994.
16. Tarasov, V.S. ed., Stremitel'nyy vzlyot, St. Petersburg Technical University, 1995.
17. Sorokin K.E. "Yadernoe oruzhie v epokhu geopolticheskoy mnogopolyarnosti," Polis, no. 4, 1995.
18. Col. Gen.Yesin V.I., ed. Sozdateli raketno-yadernogo oruzhiya i veterany-raketchiki rasskazyvayut. Moscow, TSI PK, 1996, pp. 24-39, 98, 134, 142-147.
19. Maslyukov Y.S. "U dogovora SNV-2 poyavilsya shans," Nezavisimoye voyennoye obozreniye, no. 21, June 5-18, 1996.
20. Maj. Gen. Ryaboshapko V.A. (ret.), "Usloviya perekhoda k vozmozhnomu primeneniyu yadernogo oruzhiya," Voenaya mysl,' no. 4, July-August 1996.
21. Col. Gen. Baryn'kin, V.M., "Problemy razvitiya sistemy upravleniya na sovremennom etape," Voennaya mysl', July-August 1996.
22. Yarynich V.E. "The role of command system of nuclear weapons in the strengthening of strategic stability." "Russia: in search of strategy of security. The problems of security, arms limitations and peacekeepers." IMEMO RAN, CGMF, (in Russian), 1996, pp. 45-55.
23. Nezavisimoye voyennoye obozreniye, Oct. 30, 1998.
24. Podvig P.L., ed., Strategicheskoe yadernoe vooruzhenie Rossii, Moscow, IzdAT, 1998, pp. 37-54, 128-135, 215-237, 309-311.

25. Karpenko A.V., Utkin A.F., Popov A.D., Otechestvennye strategicheksie raketnye kompleksy, St. Petersburg, Nevskiy Bastion, 1999, pp. 19-33, 207.

26. Pervov M.A. Raketnoe oruzhie Raketnykh voysk strategicheskogo naznacheniya. Moscow, National Press Institute, 1999, pp. 172-173, 227, 234.

27. Yadernyy kontrol', November 1999.

28. Izvestiya, Nov. 12, 1999.

29. Nezavisimoye voyennoye obozreniye, Dec. 17, 1999.

30. Nezavisimoye voyennoye obozreniye, Aug. 20, 1999.

Endnotes

1 Arbatov, Aleksei, *Bezopasnost'. Rossiyskiy vybor*, Moscow: EPItsentr, 1999, p. 351.

2 Blair, Bruce G., *Strategic Command and Control. Redefining the Nuclear Threat*, Washington, D.C.: Brookings Institution, 1985, p. 3.

3 Carter A., Steinbruner J. and Zraket C., *Managing Nuclear Operations*, Washington, D.C.: Brookings Institution, 1987, p. 117.

4 *Zapis' osnovnogo soderzhaniya konsul'tatsiy,* A. A. Obukhova with R. Bartholomew, Oct. 7, 1991. I would like to thank Dr. Nikolai Sokov for providing me with this document.

5 At that time, Soviet President Mikhail Gorbachev was planning to establish strategic defensive forces, embracing the SNF, BMD and space troops.

6 *Zapis' osnovnogo soderzhaniya konsul'tatsiy,* A. A. Obukhova with R. Bartholomew, Nov. 25-27, 1991.

7 Ball, Desmond, *Soviet Strategic Command, Control, Communications and Intelligence (C3I) System*, Canberra: The Strategic and Defense Studies Centre, Australian National University, 1985, p. 119.

8 Blair, Bruce G., *Global Zero Alert for Nuclear Forces*, Washington, D.C.: Brookings Institution, 1995, p. 60.

9 *Yaderny kontrol'*, November 1999.

10 *Nezavisimoye voyennoye obozreniye*, no. 49, Dec. 17, 1999.

11 "Kontseptsiya natsional'noy bezopasnosti Rossiyskoy Federatsii," *Nezavisimoye voyennoye obozreniye*, no. 001, Jan. 14, 2000.

12 Georgy A. Arbatov, "The American Strategic Debate: A Soviet View," *Survival* vol. 16 (May-June 1974), pp. 133-134, cited in Ball, Desmond, "Soviet Strategic Planning and the Control of Nuclear War," *The Soviet Calculus of Nuclear War,* Ed. Roman Kolkowicz and Ellen P. Mickiewicz, 1986. (pp. 49-67).

13 Ford, Daniel F., *The Button: The Pentagon's Strategic Command and Control System*, New York, NY: Simon and Schuster, 1985, p. 102.

14 Lt. Gen. N. Ye. Solovtsov and Maj. Gen. V.T. Nosov, *Voenaya mysl'* no. 9 (November/December 1994), p. 75.

15 A. Arbatov, *Bezopasnost'. Rossiyskiy vybor*, pp. 343-344.

16 *Ibid.*, pp. 344-345.

17 Ford, *The Button: The Pentagon's Strategic Command and Control System,* p. 91.

18 In 1992, when the SNF were located throughout Russia, Ukraine, Kazakhstan and Belarus, an agreement was reached within the CIS on consultations prior to the use of strategic forces. It has not been cancelled yet.

19 Pavel Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, Moscow: IzdAT, 1998, pp. 53, 57.

20 Blair, *Global Zero Alert for Nuclear Forces*, p. 43.

21 *Ibid.*, pp. 30-31.

22 *Ibid.*, pp. 61-62.

23 *Project Air Force Annual Report, Fiscal Year 1992*, AR-3800-af, The RAND Corporation, p. 28.

24 K.E. Sorokin, "Yadernoe oruzhie v epokhu geopolticheskoy mnogopolyarnosti," *Polis* no. 4 (1995), p. 22.

25 Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 363-368.

26 Col. Gen. V. M. Baryn'kin, "Problemy razvitiya sistemy upravleniya na sovremennom etape," *Voennaya mysl'* (July/August 1996).

27 A. Arbatov, pp. 437-438.

28 *Nezavisimoye voyennoye obozreniye* no. 49 (Dec. 17, 1999).

[29] A. A. Obukhova with R. Bartholomew, *Zapis' osnovnogo soderzhaniya konsul'tatsiy*, Oct. 7, 1991.

[30] Peter Feaver, "Command and Control in Emerging Nuclear Nations," *International Security* vol. 17, no. 3, (1992-1993), pp. 183-185.

[31] Sorokin, "Yadernoe oruzhie v epokhu geopolticheskoy mnogopolyarnosti," p. 27.

[32] Ball, Desmond, "Soviet Strategic Planning and the Control of Nuclear War," *The Soviet Calculus of Nuclear War*, pp. 49-67.

[33] Blair, *Global Zero Alert for Nuclear Forces*, p. 275.

[34] A. Arbatov, *Bezopasnost'*, p. 358.

[35] Sergei Sokut, "Effektivnost', stoimost' realizuemost'," *Nezavisimoye voyennoye obozreniye*, Oct. 30, 1998.

[36] Mikhail Pervov, *Raketnoe oruzhie raketnykh Voysk Strategicheskogo Naznacheniya*, Moscow: National Press Institute, 1999, p. 173.

[37] Gottemoeller, Rose E., "Soviet Arms Control Decision Making Since Brezhnev," *The Soviet Calculus of Nuclear War*, Ed. Roman Kolkowicz and Ellen Propper Mickiewicz, Massachusetts/Toronto: Lexington Books, D.C. Heath and Company/Lexington, 1984. (pp. 85-113.)

[38] Blair, *Strategic Command and Control: Redefining the Nuclear Threat*, p. 3.

[39] John Erickson, "Soviet Command and Control," *Military Review* vol. 52, no. 1 (January 1972), pp. 41-50.

[40] Garthoff, Raymond L., *The Soviet High Command and General Staff*, Santa Monica, CA: The RAND Corporation, 1955, p. 684.

[41] Daniel Goure, "C3 and the New Soviet Nuclear Forces," *Signal* vol. 41, no. 4 (December 1986), pp. 86-89.

[42] J. Hemsley, "Command Technology: Voennaya Sistemotekhnika. An Algorithmic Approach to Decision-making," *RUSI Journal* vol. 125, no. 3 (September 1980), pp. 58-64.

[43] Steven J. Zaloga, "Former Soviet ABM Chief Mocks USSR's Ballistic Missile Defense," *Armed Forces Journal International* (October 1990), p. 29.

[44] G. Jacobs, "Soviet Strategic Command and Control and the Tu-142 'Bear J'," *Jane's Soviet Intelligence Review* vol. 3 (April 1991).

[45] Blair, Bruce G., *The Logic of Accidental Nuclear War*, Washington, D.C.: Brookings Institution, 1993; Blair, *Global Zero Alert for Nuclear Forces*.

[46] Woods, Stan, "Weapons Acquisition in the Soviet Union," *The Soviet Calculus of Nuclear War*, Eds. R. Kolkowicz and E.P. Mickiewicz, 1986. (pp. 236-237).

[47] Ball, Desmond. "Soviet Strategic Planning and the Control of Nuclear War," *The Soviet Calculus of Nuclear War*, Eds. R. Kolkowicz and E.P. Mickiewicz, p. 63.

[48] *Ibid.*, p. 61.

[49] Blair, *The Logic of Accidental Nuclear War*; *Targeting and Deterrence*, London: IISS, 1992; Blair, *Global Zero Alert for Nuclear Forces*; Blair, Bruce G. *Strategic Command and Control: Redefining the Nuclear Threat*, Washington, D.C.: Brookings Institution, 1985; Bracken, Paul, *The Command and Control of Nuclear Forces*, Yale University Press, 1983; Ford, Daniel F., *The Button: The Pentagon's Strategic Command and Control System*, New York, NY: Simon and Schuster, 1985; Pry, Peter V. *The Strategic Nuclear Balance – Volume 1: And Why it Matters* , New York, NY: Taylor & Francis, 1990; Pry, Peter V. *The Strategic Nuclear Balance – Volume 2: Nuclear Wars Exchanges and Outcomes*, New York, NY: Taylor & Francis, 1990; Lebow, Richard Ned, *Between Peace and War: The Nature of International Crisis*, Johns Hopkins University Press, 1981; Sagan, Scott D., *Moving Targets: Nuclear Strategy and National Security*, Princeton University Press, 1989.

[50] Ball, Desmond, *Politics and Force Levels: The Strategic Missile Program of the Kennedy Administration*, University of California, 1980; *Targeting for Strategic Deterrence*, London: IISS, Summer 1983; "U.S. Strategic Forces: How Would They Be Used?" *International Security* vol.7 (Winter 1982-83); Ball, Desmond and Richelson, Jeffrey, *Strategic Nuclear Targeting*, Cornell University, 1986; Reed, Thomas C., "The Role of Nuclear Weapons in the New World Order," Briefing for the Joint Strategic Target Planning Staff/Strategic Advisory Group, Strategic Deterrence Study Group, Oct. 10, 1991.

[51] Stein, Peter and Feaver, Peter, *Assuring Control of Nuclear Weapons: The Evolution of Permissive Action Links*, Lanham, MD: University Press of America, 1987; Cotter, Donald R., "Peace Time Operations: Safety and Security," Eds. Ashton B. Carter, John D. Steinbruner, and Charles A. Zraket, *Managing Nuclear Operations*, Washington, D.C.: Brookings Institution, 1987. (pp. 17-74); Dan Caldwell, "Permissive Action Links: A Description and Proposal," *Survival* vol.29 (May-June 1987), pp. 224-38.

[52] Blair, *The Logic of Accidental Nuclear War*, p. 316.

53 Blair, *Global Zero Alert for Nuclear Forces*, p. 107.

54 John D. Steinbruner, "Launch under Attack," *Scientific American* vol. 250 (January 1984); Blair, *The Logic of Accidental Nuclear War; Targeting and Deterrence*; Blair, *Global Zero Alert for Nuclear Forces; Strategic Command and Control: Redefining the Nuclear Threat*; Betts, Richard K., *Surprise Attack: Lessons for Defense Planning*, Washington, D.C.: Brookings Institution, 1982; Betts, *Nuclear Blackmail and Nuclear Balance*, Washington, D.C.: Brookings Institution, 1987; Richard L. Garwin, "Launch under Attack to Redress Minuteman Vulnerability?" *International Security* vol. 4 (Winter 1979-80), p. 117.

55 Pate-Cornell, Elisabeth M., and Fischbeck, Paul S., *Bayesian: Updating of the Probability of Nuclear Attack*, Stanford University, Center for International Security and Arms Control, November 1990; Blair, Bruce G., and Steinbruner, John D., *The Effects of Warning on Strategic Stability*, Washington, D.C.: Brookings Institution, 1991; Steinbruner, John D., *The Cybernetic Theory of Decision: New Dimension of Political Analysis*, Princeton, NJ: Princeton University Press, 1974; Carter, A., Steinbruner, J. and Zraket, C., *Managing Nuclear Operations*, Washington, D.C.: Brookings Institution, 1987; Lebow, *Between Peace and War: The Nature of International Crisis*; Bracken, *The Command and Control of Nuclear Forces*; Betts, *Nuclear Blackmail and Nuclear Balance*; Blair, *The Logic of Accidental Nuclear War*; Blair, *Strategic Command and Control: Redefining the Nuclear Threat*; Ed. Quade, E.S., *Analysis for Military Decisions*, Santa Monica, CA: The RAND Corporation, 1964.

56 Freedman, Lawrence, *The Evolution of Nuclear Strategy*, New York, NY: St. Martin's Press, 1983, p. 181.

57 *Ibid.*, p. 180.

58 *Ibid.*, p. 181.

59 Blair, *Strategic Command and Control: Redefining the Nuclear Threat*, p. 5.

60 K. E. Sorokin, "Yadernoe oruzhie v epokhu geopolticheskoy mnogopolyarnosti," *Polis* no. 4 (1995), p. 18.

61 *Ibid.*

62 Lt. Col. G. A. Kuznetsov and Maj. S. P. Strelyaev, "Mnogopolyarnyy mir I voprosy dostatochnosti SNV," *Voennaya mysl'* no. 3 (May-June 1995).

63 *Ibid.*, p. 38.

64 *Ibid.*

65 *Ibid.*, p. 39.

66 *Ibid.*

67 *Ibid.*, p. 41.

68 *Ibid.*, p. 41.

69 Blair, *The Logic of Accidental Nuclear War.*

70 *Ibid.*, p. 20.

71 *Ibid.*, p. 280.

72 *Ibid.*, p. 285.

73 *Ibid.*, pp. 284-285.

74 Blair, *Global Zero Alert for Nuclear Forces*, p. 19.

75 Blair, *The Logic of Accidental Nuclear War*, p. 285.

76 *Ibid.*, p. 284.

77 *Ibid.*, p. 170.

78 *Ibid.*, p. 173.

79 *Ibid.*, p. 274.

80 *Ibid.*, p. 170.

81 *Ibid.*, p. 16.

82 *Ibid.*

83 *Ibid.*, p. 3.

84 *Ibid.*, p. 18.

85 *Ibid.*, p. 138.

86 *Ibid.*, p. 140.

87 *Ibid.*, p. 143.

88 *Ibid.*, p. 118.

89 *Ibid.*, p. 259.

90 Ford, *The Button: The Pentagon's Strategic Command and Control System.*

91 *Ibid.*, p. 40.

92 *Ibid.*, pp. 87-88. The author quotes the 1983 remarks by Charles Zraket of the MITRE Corporation.

93 *Ibid.*, p. 24.

94 Quade, Ed., *Analysis for Military Decisions.*

95 Bracken, *The Command and Control of Nuclear Forces.*

96 Wohlstetter, Albert, "Analysis and Design of Conflict Systems," *Analysis for Military Decisions*, Ed. Quade, pp. 135-136.

97 *Ibid.*, p. 136.

98 *Ibid.*

99 *Ibid.*

100 T. C. Schelling, "Assumptions about Enemy Behavior," *Analysis for Military Decisions*, Ed. Quade, p. 199.

101 Bracken, *The Command and Control of Nuclear Forces.*

102 *Ibid.*, p. 99.

103 *Ibid*, p. 128.

104 A. Arbatov, *Bezopasnost'. Rossiyskiy vybor*, p. 342.

105 *Ibid.*

106 *Ibid.*

107 Carter, A., Steinbruner, J. and Zraket, C., *Managing Nuclear Operations*, 1987, pp. 611-639.

108 *Ibid.*, p. 612.

109 *Ibid.*, p. 619.

110 *Ibid.*, p. 620.

111 *Ibid.*, p. 624.

112 *Ibid.*, p. 639.

113 Yarynich, V.E., *Otsenka garantii*, Moscow: MGIMO, 1994.

114 Quade, Ed., *Analysis for Military Decisions.*

115 "Command and Control of Soviet Nuclear Weapons: Dangers and Opportunities Arising from the August Revolution," Hearing before the subcommittee on European affairs of the Committee on Foreign Relations, U.S. Senate, 102nd Congress, first session, Sept. 24, 1991.

116 Tarasov, V.S., ed., *Stremitel'nyy vzlyot*, St. Petersburg Technical University, 1995; Mikhail Pervov, *Raketnoe oruzhie raketnykh Voysk Strategicheskogo Naznacheniya*, Moscow, National Press Institute, 1999, p. 172.

117 On NII AA, LPI Design Bureau, and the competition between them, see Tarasov, Ed., *Stremitel'nyy vzlyot*; A.V. Karpenko, A.F. Utkin and A.D. Popov, *Otechestvennye strategicheksie Raketnye kompleksy*, St. Petersburg, Nevskiy Bastion, 1999, pp. 22-23; Pervov, *Raketnoe oruzhie raketnykh Voysk Strategicheskogo Naznacheniya*, pp. 172-173.

118 Igor Sutyagin, "The Use of Force, Nuclear Weapons, and Civil-Military Relations in the Soviet Union and Russia: Civil-Military Relations and Nuclear Weapons," Center for International Security and Arms Control, Stanford University, June 1994, pp. 111-138; Blair, *The Logic of Accidental Nuclear War*, Index; Blair, *Global Zero Alert for Nuclear Forces*, Index.

119 Tarasov, Ed., *Stremitel'nyy vzlyot*; Army Gen. Yu. Maksimov, Ed., *Raketnye Vyska Strategicheskogo Naznacheniya*, Moscow, 1992; Col Gen. Viktor Yesin, Ed., *Sozdateli raketno-yadernogo oruzhiya i veterany-raketchiki rasskazyvayut*, Moscow: TSI PK, 1996.

120 Maksimov, Ed., *Raketnye Voyska Strategicheskogo Naznacheniya*, p. 81; Blair, *Global Zero Alert for Nuclear Forces*, Index; Tarasov, Ed., *Stremitel'nyy vzlyot*, pp. 88-97, 104, 148-151.

121 Karpenko, Utkin, Popov, *Otechestvennye Strategicheksie Raketnye Kompleksy*, p. 24; Pervov, *Raketnoe oruzhie Raketnykh voysk strategicheskogo naznacheniya*, p. 173.

122 Maksimov, Ed., *Raketnye voyska strategicheskogo naznacheniya*, p. 156; Blair, *Global Zero Alert for Nuclear Forces*, Index; Tarasov, Ed., *Stremitel'nyy vzlyot*, p. 105.

[123] Karpenko, Utkin, Popov, *Otechestvennye strategicheksie Raketnye kompleksy*, p. 31.

[124] Igor Sutyagin, "The Use of Force, Nuclear Weapons, and Civil-Military Relations in the Soviet Union and Russia: Civil-Military Relations and Nuclear Weapons," Center for International Security and Arms Control, Stanford University, June 1994, pp. 111-138, 145; Blair, *Global Zero Alert for Nuclear Forces*, Tarasov, Ed., *Stremitel'nyy vzlyot*; Pervov, *Raketnoe oruzhie raketnykh Voysk Strategicheskogo Naznacheniya*, p. 173.

[125] Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, p. 235; Blair, *The Logic of Accidental Nuclear War*, p. 157; Karpenko, Utkin, Popov, *Otechestvennye strategicheskie Raketnye komplesky*; Pervov, *Raketnoe oruzhie raketnykh Voysk Strategichesko Naznacheniya*, Ministry of Defense, Peter the Great Military Academy, 1999; *Voennyy entsiklopedicheskiy slovar' raketnykh Voysk Strategicheskogo Naznacheniya*, Ministry of Defense, Peter the Great Military Academy, 1999.

[126] Tarasov, Ed., *Stremitel'nyy vzlyot*.

[127] Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, p. 235; Blair, *The Logic of Accidental Nuclear War*, p. 157.

[128] Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, p. 235.

[129] Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, p. 235; Blair, *The Logic of Accidental Nuclear War*, Index.

[130] Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, p. 215, 230-237.

[131] Information about the designers of command and control systems for the airborne strategic nuclear forces can be found in Tarasov, V.S. Ed., *Stremitel'nyy vzlyot*; Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 309-311; Blair, *The Logic of Accidental Nuclear War*, pp. 76, 165.

[132] Information about the command posts of the top echelons of the command of the Armed forces of Russian Federation can be found in Yesin, Ed. *Sozdateli raketno-yadernogo oruzhiya i veterany-raketchiki rasskazyvayut*, pp. 28-39; *Voennyy entsiklopedicheskiy slovar' raketnykh Voysk Strategicheskogo Naznacheniya*; Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 45, 52-54; Sutyagin, "The Use of Force, Nuclear Weapons, and Civil-Military Relations in the Soviet Union and Russia: Civil-Military Relations and Nuclear Weapons," pp. 111-138; Blair, *The Logic of Accidental Nuclear War*, pp. 78, 141-150, 163-165.

[133] Much has been published recently about the *Kazbek*, it was even the subject of newspaper articles and TV programs. See Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 50, 378; Sutyagin, "The Use of Force, Nuclear Weapons, and Civil-Military Relations in the Soviet Union and Russia: Civil-Military Relations and Nuclear Weapons," pp. 111- 138; Blair, *The Logic of Accidental Nuclear War*, Index; Blair, *Global Zero Alert for Nuclear Forces*, Index.

[134] Podvig, *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 50, 378; Igor Sutyagin, "O diskussi po povodu planov sozdaniya OGK SSS: ne vsyo tak odnoznachno," Moscow: Center for Study of Arms Control, Energy and Ecology, Moscow Physical Technical Institute, March 15, 1999; Sutyagin, "The Use of Force, Nuclear Weapons, and Civil-Military Relations in the Soviet Union and Russia: Civil-Military Relations and Nuclear Weapons," p. 127; Blair, *Global Zero Alert for Nuclear Forces*, Index.

[135] Sutyagin, "The Use of Force, Nuclear Weapons, and Civil-Military Relations in the Soviet Union and Russia: Civil-Military Relations and Nuclear Weapons," pp. 111-138; Blair, *Global Zero Alert for Nuclear Forces*, Index; Sutyagin, "O diskussi po povodu planov sozdaniya OGK SSS: ne vsyo tak odnoznachno."

[136] "Command and Control of Soviet Nuclear Weapons: Dangers and Opportunities Arising from the August Revolution," Hearing before the Subcommittee on European Affairs of the Committee on Foreign Relations, U.S. Senate, 102nd congress, first session, Sept. 24, 1991.

[137] The SRF, Air Force, and Navy.

[138] "Command and Control of Soviet Nuclear Weapons: Dangers and Opportunities Arising from the August Revolution," Hearing before the Subcommittee on European Affairs of the Committee on Foreign Relations, U.S. Senate, 102nd congress, first session, Sept. 24, 1991, p. 5.

[139] The algorithm of launch operations in the Russian C^3 system is also described in Podvig, ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 50-54.

[140] *Izvestiya*, Nov. 12, 1999.

[141] About the *Signal* system, see Maksimov, Ed., *Raketnye Voyska Strategicheskogo Naznacheniya*, pp. 83, 123-126; Hemsley, J., "Command Technology: Voennaya Sistemotekhnika: An Algorithmic Approach to Decision-making," pp. 58-64, Index; Tarasov, Ed., *Stremitel'nyy vzlyot*; Col Gen. Viktor Yesin, Ed., *Sozdateli raketno-yadernogo oruzhiya I veterany-raketchiki rasskazyvayut*, Moscow: TSI PK, 1996, p. 142; Yuri Maslyukov, "U dogovora SNV-2 poyavilsya shans," *Nezavisimoye voyennoye obozreniye* no. 21 (June 5-18, 1996); Blair, *The Logic of Accidental Nuclear War*, pp. 76, 100, 145, Index.

[142] For the latter type of publications, see "Command and Control of Soviet Nuclear Weapons: Dangers and Opportu-

nities Arising from the August Revolution," Hearing before the Subcommittee on European Affairs of the Committee on Foreign Relations, U.S. Senate, 102nd Congress, first session, Sept. 24, 1991; Maksimov, Ed., *Raketnye Voyska Strategicheskogo Naznacheniya*, p. 156; Blair, *The Logic of Accidental Nuclear War*, Index; Blair, Bruce G., "Russia's Doomsday Machine," *The New York Times*, Oct. 8, 1993, p. 17; Sutyagin, "The Use of Force, Nuclear Weapons, and Civil-Military Relations in the Soviet Union and Russia: Civil-Military Relations and Nuclear Weapons," pp. 111-138; Blaii, *Global Zero Alert for Nuclear Forces*, Index; Yuri Maslyukov, "U dogovora SNV-2 poyavilsya shans," *Nezavisimoye voyennoye obozreniye* no. 21 (June 5-18, 1996); Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 52-53.

143 Karpenko, Utkin, Popov, *Otechestvennye strategicheksie Raketnye kompleksy*.

144 Frequently, strategic systems were put on combat watch before passing formal acceptance tests because of the arms race pressure.

145 Karpenko, Utkin, Popov, *Otechestvennye strategicheksie Raketnye kompleksy*, p. 207.

146 *Voennyy entsiklopedicheskiy slovar' Raketnykh Voysk Strategicheskogo Naznacheniya* (Moscow: Ministry of Defense, Peter the Great Military Academy, 1999, pp. 626-629.

147 Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, p. 57.

148 Conditions for combat actions by the crews of radio command and control centers, as well as the information about command missiles, can be found in Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 52-53.

149 On command and control of divisions of silo-based and mobile ICBMs, see Karpenko, Utkin, Popov, *Otechestvennye strategicheksie Raketnye kompleksy*, pp. 19-33; Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 131, 150-154; Maksimov, Ed. *Raketnye Voyska Strategicheskogo Naznacheniya*; Yesin,Ed. *Sozdateli raketno-yadernogo oruzhiya I veterany-raketchiki rasskazyvayut*; Blair, *The Logic of Accidental Nuclear War*; Blair, *Global Zero Alert for Nuclear Forces*; Pervov, *Raketnoe oruzhie Raketnykh Voysk Strategicheskogo Naznacheniya*, pp. 173, 227, 234.

150 *Izvestiya*, Nov. 12, 1999.

151 Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, p. 234; Blair, *The Logic of Accidental Nuclear War*, pp. 129, 157.

152 Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 128-130, 221-227; Maksimov, Ed., "Raketnye Voyska Strategicheskogo Naznacheniya;" Tarasov, Ed., *Stremitel'nyy vzlyot*; Yesin, Ed., *Sozdateli raketno-yadernogo oruzhiya I veterany-raketchiki rasskazyvayut*.

153 About military representatives (*voenpredy*), see Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, p. 37.

154 On some of the former and currently operating defense industrial enterprises that have contributed to building a strategic C^3 system, see Maksimov, Ed., "Raketnye Voyska Strategicheskogo Naznacheniya," pp. 82, 157; Tarasov, Ed., *Stremitel'nyy vzlyot*, pp. 88-97; Yesin, Ed., *Sozdateli raketno-yadernogo oruzhiya I veterany-raketchiki rasskazyvayut*, pp. 28-39, 134, 142-147; Karpenko, Utkin, Popov, *Otechestvennye strategicheksie Raketnye kompleksy*, pp. 24, 31; Pervov, *Raketnoe oruzhie Raketnykh Voysk Strategicheskogo Naznacheniya*.

155 Woods, Stan, *Weapons Acquisition in the Soviet Union*, Eds. R. Kolkowicz and E.P. Mickiewicz, "The Soviet Calculus of Nuclear War," 1986, p. 222.

156 *Ibid.*, p. 222.

157 *Ibid.*, p. 225.

158 *Ibid.*, p. 218

159 Tarasov, *Stremitel'nyy vzlyot*, p. 136.

160 Woods, *Weapons Acquisition in the Soviet Union;* R. Kolkowicz and E.P. Mickiewicz, Eds., "The Soviet Calculus of Nuclear War," p. 232.

161 For a sufficiently detailed description of the system of weapons R&D and production in the USSR and Russia, see Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 37-40, 135-150.

162 Tarasov, Ed., *Stremitel'nyy vzlyot*, p. 5.

163 Col. Gen. I. D. Sergeyev, "Sovershenstvovanie boevoy gotovnosti Raketnykh voysk strategicheskogo naznacheniya v usloviyakh realizatsii dogovoro po SNV," *Voennaya mysl'* no.6 (November-December 1995), p. 19.

164 Col. Gen. V. M. Baryn'kin, "Problemy razvitiya sistemy upravleniya na sovremennom etape," *Voennaya mysl'* (July-August 1996), p. 31.

165 Blair, *Global Zero Alert for Nuclear Forces*, p. 73.

166 Blair, *The Logic of Accidental Nuclear War*, p. 112.

167 Some information on operational planning of Russia's SNF can be found in Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 45-47.

168 Pry, *The Strategic Nuclear Balance. Volume 2: Nuclear Wars: Exchanges and Outcomes*, p. 23.

169 *Ibid.*, p. 27.

170 *Ibid.*, p. 29.

171 Blair, *The Logic of Accidental Nuclear War*, pp. 328-329.

172 Pry, *The Strategic Nuclear Balance. Volume 2: Nuclear Wars: Exchanges and Outcomes*, p. 26

173 See, for instance, Blair, "Strategic Command and Control;" Pry, *The Strategic Nuclear Balance. Volume 2: Nuclear Wars: Exchanges and Outcomes*; Ford, "The Button: The Pentagon's Strategic Command and Control System;" Babbit, Albert E. "Command Centers," *Managing Nuclear Operations*, Brookings Institution, 1987; Savage, Paul L., *Strategic Nuclear War: What the Superpowers Target and Why*, Greenwood Press, New York, 1986.

174 Blair, *Strategic Command and Control*, p. 241.

175 Sagan, Scott D., "Moving Targets: Nuclear Strategy and National Security," Princeton, NJ: Princeton University, 1989, p. 9.

176 Blair, *Strategic Command and Control*, p. 243.

177 *Ibid.*, pp. 243-244.

178 *Ibid.*, pp. 7, 246.

179 Coakley, Thomas P., "Command and Control for War and Peace," Washington, D.C.: National Defense University Press, 1991, p. 43.

180 Blair, *Strategic Command and Control*, p. 243.

181 Sergeev, Col. Gen. I.D., "Sovershenstvovanie boevoi gotovnosti Raketnikh Voisk Strategicheskovo Naznacheniya v usloviakh realizatsii dogovorov po SNV," *Voennaya Mysl'* no. 6 (November-December 1995), Moscow.

182 Woods, "Weapons Acquisition in the Soviet Union," *The Soviet Calculus of Nuclear War*, p. 207.

183 Blair, *Strategic Command and Control*, p. 279.

184 *Ibid.*, p. 281.

185 *Ibid.*

186 Blair, *The Logic of Accidental Nuclear War*, p. 107.

187 *Ibid.*, p. 90.

188 *Ibid.*, pp. 98-99

189 *Ibid.*, p. 97

190 Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, p. 237.

191 Blair, *The Logic of Accidental Nuclear War*, p. 278.

192 Carter, A., Steinbruner, J. and Zraket, C., Eds., *Managing Nuclear Operations*, p. 46.

193 Blair, *The Logic of Accidental Nuclear War*, p. 279

194 *Ibid.*, p. 279

195 *Ibid.*

196 Carter, A., Steinbruner, J., and Zraket, C., Eds., *Managing Nuclear Operations*, p. 53.

197 "Command and Control of Soviet Nuclear Weapons: Dangers and Opportunities Arising from the August Revolution." Hearings before the Subcommittee on European Affairs of the Committee on Foreign Relations of the U.S. Sentate. 102nd Congress, 1st session, Sept. 24, 1991; pp. 10, 22.

198 Blair, *The Logic of Accidental Nuclear War*, p. 82.

199 *Ibid.*, p. 82.

200 Ball, "Soviet Strategic Command, Control, Communications and Intelligence (C^3I) System," p. 143.

201 Blair, *The Logic of Accidental Nuclear War*, pp. 84-86.

202 Blair, *Global Zero Alert for Nuclear Forces*, p. 49.

203 Blair, *The Logic of Accidental Nuclear War*, p. 85.

204 "Command and Control of Soviet Nuclear Weapons: Dangers and Opportunities Arising from the August Revolution," Hearing before the Subcommittee on European Affairs of the Committee on Foreign Relations, U.S. Senate, 102nd congress, first session, Sept. 24, 1991, p. 22.

205 Blair, *The Logic of Accidental Nuclear War*, p. 112.

[206] Sagan, "Moving Targets: Nuclear Strategy and National Security," p. 118.

[207] Pry, "The Strategic Nuclear Balance," *Exchanges and Outcomes, Volume 2: Nuclear Wars.*

[208] *Ibid.*, p. 17.

[209] Speed, Roger D., *Strategic Deterrence in the 1980s*, Stanford, CA: Hoover Institution, 1979, p. 69.

[210] Blair, Bruce G., "Alerting in Crisis and Conventional War," *Managing Nuclear Operations*, Eds. Carter, Ashton B., Steinbruner, John D., Zraket, Charles A., Washington, D.C.: Brookings Institution, 1987, pp. 107-108.

[211] Blair, Bruce, G., *Strategic Command and Control: Redefining the Nuclear Threat*, Washington, D.C.: Brookings Institution, 1985, p. 226.

[212] *Ibid.*, p. 271.

[213] Blair, *The Logic of Accidental Nuclear War*, p. 136.

[214] *Ibid.*, p. 137.

[215] *Ibid.*, p. 140.

[216] *Ibid.*, p. 143.

[217] *Ibid.*, p. 145.

[218] *Ibid.*, p. 150.

[219] *Ibid.*, p. 163.

[220] *Ibid.*, p. 163.

[221] *Ibid.*, p. 166.

[222] Samokhvalov, Plotnikov, "Problemy ispol'zovaniya novykh informatsionnykh tekhnologiy v upravlenii voyskami," *Voennaya mysl'* no. 4 (July-August 1996), p. 41.

[223] "U.S.-Russian Strategic Missiles Detargeting Complete," *Arms Control Today* (July-August 1994), p. 26.

[224] Blair, *Global Zero Alert for Nuclear Forces*, p. 79.

[225] Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, p. 152.

[226] Blair, *The Logic of Accidental Nuclear War*, pp. 219-254.

[227] *Ibid.*, pp. 251-252.

[228] Paul Podvig, "The Operational Status of the Russian Space-Based Early Warning System," *Science and Global Security* vol. 4 (1994) pp. 370-371.

[229] See Podvig, Ed., *Strategicheskoe yadernoe vooruzhenie Rossii*, pp. 42-44.

[230] There is an interesting discrepancy in the American and Russian terminology. In the American terminology, we usually refer to two different postures: launch-on-warning and launch-under-attack. Russians frequently have three distinct terms to describe nuclear postures. *Vstrechnyy udar* (a meeting strike, like meeting engagement in conventional military terminology) is a strike delivered only in response to data obtained by the EWS, and thus is an equivalent of the American launch-on-warning. *Otvetno-vstrechnyy udar* (a retaliatory/meeting strike) is launched as soon as sensors record the first nuclear detonations on friendly territory, before an assessment of the enemy strike can be performed. *Otvetnyy udar* (a retaliatory strike) is launched only after a post-attack assessment is completed; it's most precise English equivalent is delayed second strike. For the sake of convenience, we refer to the second and third scenarios as launch-under-attack, unless it is necessary to specifically refer to delayed second strike.

[231] Kartchner, Kerry M., "The Objectives of Arms Control," *Arms Control: Toward the 21st Century,* Eds. Larsen, Jeffrey A., Rattray, Gregory J., Boulder, CO: Lynne Rienner, 1996, p. 20.

[232] Blair, *Global Zero Alert for Nuclear Forces*, p. 56.

[233] *Ibid.*, p. 105.

[234] *Ibid.*, p. 103.

[235] *Ibid.*, p. 104.

[236] *Ibid.*, p. 100.

[237] *Ibid.*, p. 103.

[238] Sagan, *Moving Targets: Nuclear Strategy and National Security*, p. 141.

[239] Feaver, Peter D., *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States*, Ithaca, NY: Cornell University Press, 1992.

[240] *Ibid.*, p. 46.

[241] *Ibid.*, p. 47.

[242] *Ibid.*, p. 48.

[243] *Ibid.*, p. 49.

[244] *Ibid.*, p. 52.

[245] Blair, *The Logic of Accidental Nuclear War*, p. 8.

[246] Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States*, p. 54.

[247] Sagan, *Moving Targets: Nuclear Strategy and National Security*, p. 142.

[248] *Ibid.*, p. 142.

[249] Blair, *The Logic of Accidental Nuclear War*, pp. 78-80.

[250] Blair, *Global Zero Alert for Nuclear Forces*, p. 54.

[251] Blair, Bruce G., "Russia's Doomsday Machine," *The New York Times*, Oct. 8, 1993, p. 17.

[252] Blair, *The Logic of Accidental Nuclear War*, pp. 78-80, 208; "Command and Control of Soviet Nuclear Weapons: Dangers and Opportunities Arising from the August Revolution," Hearing before the Subcommittee on European Affairs of the Committee on Foreign Relations, U.S. Senate, 102nd Congress, first session, Sept. 24, 1991.

[253] Yarynich, V.E., "The Doomsday Machine's Safety Catch," *The New York Times*, Feb. 1, 1994, p. A17.

[254] Blair, *Global Zero Alert for Nuclear Forces*, p. 53.

[255] *Ibid.*, pp. 55-56.

[256] Sagan, *Moving Targets: Nuclear Strategy and National Security*, p. 4.

[257] Blair, Bruce G., "The Effects Of U.S. Policy On Russian Nuclear Control," *The Proliferation Threat of WMD and U.S. Security Interests*, The Aspen Institute Workshop, Aug. 10-15, 1996.

[258] *Ibid.*

[259] *Ibid.*

[260] Ryaboshapko, Maj. Gen. V.A. (ret.), "Usloviya perekhoda k vozmozhnomu primeneniyu yadernogo oruzhiya," *Voenaya mysl'* no. 4 (July-August 1996), pp. 10-14.

[261] Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States*, pp. 20-21.

[262] *Izvestiya*, Nov. 12, 1999.

[263] Lynn Eden and Steven E. Miller, Eds., *Nuclear Arguments. Understanding the Strategic Nuclear Arms and Arms Control Debates,* Ithaca,NY: Cornell University Press, 1989, p. 122.

[264] *Ibid.*, p. 122.

[265] *Ibid.*, p. 121.

[266] Coakley, *Command and Control for War and Peace*, p. 8.

[267] Lee Paschall, *C3I and the National Military Command System*, 1980, cited in *C3I: Issues of Command and Control*, Ed. Thomas P. Coakley, Washington, D.C.: National Defense University Press, 1991, p. 118.

[268] Sherman Frankel. "Aborting Unauthorized Launches of Nuclear-Armed Ballistic Missiles through Postlaunch Destruction," *Science and Global Security* vol. 2 (1990), pp. 1-20.

Glossary

ABM	Anti-Ballistic Missile
ABRCP	automobile-based reserve command post
ACCS	automated command and control system
ACP	airborne command post
AF	Armed Forces
AFSATCOM	Air Force Satellite Communications
ALCC	airborne launch control center
BMD	Ballistic Missile Defense
C^3	C-cube (command, control, communications)
C^3I	C-cube-I (command, control, communications, and intelligence)
CCM	complex of command missiles
CIA	Central Intelligence Agency
CIS	Commonwealth of Independent States
CP	command post
CPSU	Communist Party of the Soviet Union
CS	command system
CUD (cud)	clearly unacceptable damage
DM	decimeter range
DoD	Department of Defense
DSCS	Defense Satellite Communications System
DSS	delayed second strike
EAM	Emergency Action Message
ELF	extremely low frequency
EMP	electro-magnetic pulse
ERCS	Emergency Rocket Command System
EWS	Early Warning System
GIS	global information system
GS	General Staff
HBACP	helicopter-based airborne command post
HF	high frequency
HLMCP	high-level military command post
IC	individual channel
ICBM	intercontinental ballistic missile

JCS	Joint Chiefs of Staff
KSBU	*kcomandnaya sistema boevogo upravleniya* (combat command system)
LCC	launch control center
LF	low frequency
LOW	launch on warning
LPI	Leningrad Polytechnic Institute
LUA	launch under attack
m	mathematical expectation
MC	major channel
MF	middle frequency
MILSTAR	Military, Strategic, Tactical and Relay
MIRV	multiple independently targeted reentry vehicle
NCA	National Command Authority
NDS	nuclear delivery system
NMD	National Missile Defense
NORAD	North American Air Defense Command
NP	nuclear potential
NW	nuclear weapons
P	probability
PA	preliminary authorization
PAL	permissive action links
PAP	*pul't avtonomnogo puska* (device for launching a missile)
R&D	Research and Development
RBU	*radio-boevoe upravlenie* (RBCC; radio battle command channels)
RCC	radio command center
req.	requested
RF	Russian Federation
SA	satellite apparatus
SAC	Strategic Air Command
SB	strategic bomber
SC	satellite communications
SCF	shore communications facility
SCP	standardized command post
SDI	Strategic Defense Initiative
SIM	statistical imitation model
SINA	system for identification of nuclear attack
SLBM	submarine-launched ballistic missile
SNF	Strategic Nuclear Forces
SRF	Strategic Rocket Forces
SSBN	nuclear submarine armed with ballistic missiles
START	Strategic Arms Reduction Talks

STRATCOM	U.S. Strategic Command
TACAMO	Take Charge And Move Out
TNW	tactical nuclear weapons
UD (ud)	unacceptable damage
UHF	ultra-high frequency
UKP	*unifitsirovanny komandnyy punkt* (standard command post)
ULF	ultra-low frequency
VHF	very high frequency
VLF	very low frequency
wh	warhead
WMD	weapons of mass destruction

CDI

CENTER FOR DEFENSE INFORMATION
1779 Massachusetts Ave., NW, Washington, D.C. 20036-2109
Ph: 202.332.0600 Fax: 202.462.4559 www.cdi.org